TITLE		REF [as per register]	VERSION
Data Protection Procedures		CP021	2.0
DEPARTMENT	Risk and Resilience		
DATE	15 June 2026	**REVIEW DATE**	15 June 2028

Data Protection Procedures

Contents

1 – Introduction
2 – Glossary
3 – Key considerations
4 – Data Security
5 – Privacy Notices
6 – Lawfulness
7 – Retention
8 – Data Sharing
9 – Third Party Requests
10 – Data Transfer Outside the UK
11 – Data Subject Rights
12 – Research
13 – Student Research
14 – Automated decision-making
15 – Data Protection by Design and Default
16 – Direct Marketing
17 – Data Protection Breaches
18 – Email and Mailing Lists
19 – CCTV Guidance
20 – Photography

Appendices:

Appendix 1. Definitions
Appendix 2. Privacy Notices
Appendix 3. Generative Artificial Intelligence
Appendix 4. Sharing Personal Data
Appendix 5. Guidance on Legal Basis for Processing
Appendix 6. Specialised Guidance
Appendix 7. Personal Data Processed by Students
Appendix 8. Data Protection and Social Media
Appendix 9. Dealing with a Subject Access Request
Appendix 10. Freedom of Information Procedure
Appendix 11. Data Breach Procedure
Appendix 12. Risk Assessment Process for Data Incidents

Version number	Author/editor	Date	Edits made
1	DPO	01/08/2023	DP Handbook created
2	DPO	15/06/2026	Details of Sentry added at page 19 and Data Access and Use Act added to Glossary on page 2. Group Head of Risk and Resilience changed to Group Head of Risk and Resilience

1. Introduction

The UK General Data Protection Regulation and the Data Protection Act 2018 cover all personal data processed by Activate Learning (hereafter referred to as the College), irrespective of where the data is held and what format it is held in. The Data Protection Policy provides the scope and underlying requirement.

2. Glossary

The following terms are used within the Data Protection Handbook and the guidance documents:

The UK GDPR – UK General Data Protection Regulation

The DPA – Data Protection Act 2018

The DUAA – Data (Use and Access) Act 2025

Personal Data – Current data protection legislation applies only to personal data about a living, identifiable individual.

Special Categories of Personal Data – Personal data is classed as belonging to "special categories" under current data protection legislation if it includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- physical or mental health
- sexual life or sexual orientation
- commission of offences or alleged offences
- genetic data
- biometric data

Please note the new guidance on genetic data on the ICO website.

Data Subject – A data subject is an individual who is the subject of personal data.

Processing – Data processing is any action taken with personal data. This includes the collection, use, disclosure, destruction and holding of data.

Data Controller – A data controller is an organisation that has full authority to decide how and why personal data is to be processed, and that has the overall responsibility for the data. This includes deciding on use, storage, and deletion of the data.

Data Processor – A data processor is an organisation that processes personal data on behalf of another organisation.

Automated Decision-Making – Automated decision-making takes place where decisions are made solely by automated means without any human involvement.

Profiling – Profiling means automated processing of personal data to evaluate certain things about a person, to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, reliability, behaviour, or movements.

The detailed definitions can be found here: Definitions

3. Key considerations

Before embarking on any processing personal data, whether that be sharing personal data with a third party, using a new online tool, marketing a new programme or any other action that involves the use of personal data, you should ask yourself the following questions:

- Do you really need to use the information?
- Could anonymised or pseudonymised data be used?
- Are you sure that the personal data will be secure during the process? (see section 4)

- Has the data subject been told about the processing i.e., been issued with a privacy notice? (see section 5)
- Do you have a valid justification for processing the data i.e., it is required for a contract or has the data subject given their consent. (see section 6)
- Are you planning to pass personal data on to a third party or transfer the data outside the EEA? If so, do you have the necessary safeguards/permissions in place to do this?
- If you are setting up new systems/processes have the Data Protection by Design and Data Protection Impact Assessment guidelines been followed?
- Are there alternative ways the same objective can be achieved without using or sharing personal data?

If having considered the points above you conclude that the processing of personal information is necessary, then the information in the following sections will provide more details about the factors that need to be considered and the actions that need to be taken to ensure the processing meets the requirements of UK GDPR and the DPA.

4. Data Security

The Group Director of IE & IT (responsible for Information Security), and the Group Head of Risk and Resilience as the Data Protection are responsible for leading and owning the College information security and data protection risk strategy. They encourage a risk-based approach to provide holistic responses to information security and data protection risks. The two lead on pan-College information security and data protection initiatives, provides strategic advice on existing and emerging information security threats and delivers security awareness and data protection training to support this.

On the Information Technology and Data Protection SharePoint sites, you will find all necessary guidance, policies, and procedures to ensure that you protect the information you process appropriately. You will also find mandatory Information Security and Data Protection training you must complete.

Detailed guidance on data security can be found here:

Information Security - Keeping Safe Online

Data Protection

5. Privacy Notices

Under the 'fair and transparent' requirements of the first data protection principle, the College is required to provide data subjects with a privacy notice to let them know what we are doing with their personal data.

A privacy notice must be:

- easily accessible,
- provided at the time of collecting the data,
- written concisely

The College uses a tiered approach to privacy notices: The College website displays the Privacy Policy and provides details of why and how the College uses personal data. There are also two separate Privacy Notices relating to Students and Job Applicants. The web page also contains the information that is generic to all data processing (contact details of the DPO, data subject rights, rights to complain to the ICO). The purpose for this approach is to make the privacy notice provided to data subjects as short and easily readable as possible.

The College privacy notices can be found here:

College Privacy Notices

Where personal data is collected outside of these two situations, a separate privacy notice will be provided by the College Department collecting the data.

6. Lawfulness

Whenever the College processes personal data in any way, there must be a valid justification, a so-called legal basis (also called 'lawful Basis') for doing so. The UK GDPR and the DPA provide a list of six legal basis for personal data. If special categories of personal data are processed, the law provides an additional list of legal basis. Thus, for special categories, one legal basis from each of the two lists must be met.

The legal basis to choose from for personal data are:

- consent
- necessary for performance of a contract (e.g., the delivery of a course);
- legal obligation (e.g., statutory record keeping);
- vital interest (e.g., to save someone's life);
- necessary for the performance of public tasks/core functions (e.g., enforcement of the law); and
- necessary for a legitimate interest (as a publicly funded body, we are restricted from using this).

If you decide to use 'necessary for a legitimate interest' as your legal basis, you will have to conduct a Legitimate Interest Assessment ("LIA"). To be assigned an assessment, contact the DPO at dpo@activatelearning.ac.uk. To find out whether an LIA has already been conducted, contact the DPO at dpo@activatelearning.ac.uk.

For special categories of personal data, the relevant legal basis for the College is:

- explicit consent
- necessary for purposes of employment or social security law
- necessary for reasons of substantial public interest
- necessary for medical purposes
- necessary for archiving purposes or statistics and research.

A full description of these legal basis together with examples for their use can be found here: Guidance on Legal Basis for Processing

7. Data Retention

The UK GDPR sets a clear requirement for the College to take its data retention responsibilities seriously. Personal data should only be retained for as long as necessary. Just how long 'necessary' is, however, can differ based on the type of data processed, the purpose of processing or other factors. Not only do you have to inform data subjects in the privacy notice how long you keep their personal data for, but you will also then have to ensure that these retention times are adhered to. This means that data will need to be deleted, destroyed, or fully anonymised at the end of the retention time or archived appropriately in the College Archives.

It is important to note that on the other hand, in some circumstances personal data must be kept as destroying such data would be a data protection breach, for example the core archival student record to verify a student's qualifications.

Data retention is a personal responsibility for everybody in the College and it is important that you have an overview of where personal data is stored. This may include:

- own servers
- third party servers
- email accounts
- SharePoint sites
- Shared drives
- backup storage

- paper files

College records should always be stored in a departmental filing scheme, rather than by individuals. For example, you should not run reports and save them in spreadsheets in a folder on your desktop. Systems must be set up to make this less likely to happen in the first place. Staff should use managed desktops or connect remotely where practical.

To determine how long to retain a document containing personal data, first consult the relevant privacy notice. If the detail you require is not contained in the privacy notice, consult your business unit's data retention register. The master register can be found in SharePoint: Data Retention Register

8. Data Sharing

You may be asked to share personal data both within the College (by colleagues in your own area or in another unrelated area) and outside the College (by another organisation). Note that if you use an external company or organisation to process personal data on your behalf (a 'data processor'), the requirements for data sharing do not apply.

Internal data sharing

Internal data sharing, whether with a colleague from your own area or somebody from another unrelated area will usually be unproblematic if a data access protocol is completed and approved by the respective data steward. There are two types of data access protocols, one for one-off, ad hoc data sharing requests, and one for APIs (Application Programming Interface) or regular data dumps. The type of questions the protocols contain are:

- Would data subjects expect their data to be shared with you and is the purpose for sharing the data consistent with what the data subjects have been told in the privacy notice and do the legal basis and retention periods still apply? Would data subjects expect their data to be shared with you?

The key privacy notices can be found here:

- Privacy and Data Protection website
- Staff recruitment privacy notice
- Student privacy notice

Has a Data Protection Impact Assessment been carried out – if not, why not? (see section 15)

External data sharing

If another organisation requests that you share personal data, then you will need to ask these questions:

- Does the sharing involve the transfer of data outside the UK or the EU (European Union)? (see section 10)
- Is the third party acting as a processor for the College i.e., acting under the instruction and on behalf of the College?
- Is the third party requesting the personal data for their own use and purpose?

Then the third party is another data controller.

If you are setting up a relationship with an outside organisation that will involve the transfer of personal information, you must put in place a contract to ensure that adequate protection is given to that information so that the College meets its data protection obligations and protects the rights of the individuals involved.

There are specific contract requirements depending on the circumstances. For example, the standard terms and conditions of most cloud service providers are not normally sufficient. The DPO

can provide template agreements to meet the needs of different transfer arrangements. They can be contacted at: dpo@activatelearning.ac.uk

9. Third Party Requests

The College often receives requests for the personal information of its students and staff from third parties. Detailed guidance on sharing personal data with third parties can be found here: Sharing Personal Data

Requests from parents, friends, or relatives of a student

No release without the student's consent. It is acceptable to advise the requesters that we will accept a message and, if having checked our records and such a person exists, will pass it on. This avoids disclosing any information about the student, including whether they are at the College. More guidance can be found here: Parents and Family Members

Requests from organisations providing financial support

The College routinely notifies public funding bodies and the Student Loans Company of changes to a student's status. These disclosures are covered in our privacy notices and records of processing activities. Records should not be disclosed to organisations that are not covered in our privacy notices (e.g., private funders) without evidence of student consent.

Requests from Home Office/UK Visas and Immigration (UKVI)

The College often receives requests for information on attendance and other details relating to international students. Information should only be disclosed where we are satisfied there is a legal requirement to provide the requested information, or the individual concerned has given their consent. Requests for student information should be passed on to the DPO at dpo@activatelearning.ac.uk

Requests from the Police or law enforcement officials

The College is not legally obliged to provide information to the police, unless presented with a court order. However, the College will usually choose to release information where the police, or other law enforcement agencies, can demonstrate to our satisfaction that non-release would be likely to prejudice the prevention/detection of crime or apprehension/prosecution of offenders. For such requests, the established procedure can be found here: Police enquiries, and similar agencies

The College may receive requests for information regarding an allegation of fraud or misrepresentation as regards degree results. For such requests, guidance can be found here: Fraud or misrepresentation

Disclosures required by law

There are circumstances where the College is legally obliged to disclose information about an individual to a third party if this is required by law, enactment, or court order:

Third Party	**Authorisation for disclosure**
UK Funding Councils e.g., ESFA (Education and Skills Funding Agency), HEFCE (Higher Education Funding Council for England) HEFCW, and their agents e.g., QAA, Auditors etc	Further and Higher Education Act, 1992 s.79
Electoral registration officers	Representation of the People Act 2000; The Representation of the People (Scotland) & (England and Wales) Regulations 2001

Officers of the Department of Works and Pensions, and Local Authorities	Social Security Administration Act 1992: s.110A, s.109B and s.109C
Health and Safety Executive	RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations) 2013 s.3
Audit Commission and related auditing bodies	Audit Commission Act 1998 s.6
Environmental Health Officers	Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988
Environment Agency	Agency Regulations – specific ones to be quoted
Inland Revenue	Taxes Management Act 1970
Other third parties	With a Court Order

With such requests, we must ensure that any legal obligation (details of legislation and relevant section) is correctly described by the requestor in writing.

10. Data Transfer Outside the UK

International data transfer can be:

- Sending personal data from the College to an organisation, company or an individual that is based in a non-EEA country such as during research collaborations, for student exchange or using external examiners
- Uploading photos of individuals to the College website

These transfers are not prohibited; however, we must ensure that so-called safeguards are in place. The UK GDPR provides a list of these safeguards, one of which must apply:

Adequacy of the country: The EU has assessed the third country to have an adequate level of protection. These countries are then treated as though they were an EU member state and data can be transferred there without the need for any further safeguards. The countries that currently fall into this category are:

- Andorra
- Argentina
- Canada
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- Faroe Islands
- Japan

Since the UK has left the EU, the adequacy decision for these countries will be adopted by the UK, and all EEA countries will be considered adequate.

Transfers to the USA: The decision by the European Court of Justice from July 2020 invalidated the Privacy Shield for data transfer to the US and added requirements for use of the standard contractual to be inserted into contracts.

Standard Contract Clauses: If you have a contract with the organisation, you are sending the data to, it must include specific data protection contract clauses. Information and templates of these clauses for insertion into the contract can be obtained from the DPO at dpo@activatelearning.ac.uk

Additionally, a risk assessment must be completed and approved by the GET Sponsor or their representatives whenever these clauses are to be used. This risk assessment is contained in one of the questions in the DPIA.

Court orders: You have received a court order requiring the transfer.

Consent: The data subject has given explicit consent to the transfer, having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards. Where transfers are done based on consent, evidence of the consent and when it was obtained should be kept.

Contract with the data subject or in the interest of the data subject: The transfer is necessary for a contract between the data subject and the College, for example when non-EEA students ask for their exam results to be sent to their funding organisation in their home country. When students wish to spend a term abroad, there will be a contract between the College and the host organisation, and that contract is in the interest of the students.

Public interest: The transfer is necessary for important reasons of public interest.

Examples for this are crime prevention and detection, or national security.

Lawsuits: The transfer is required for a lawsuit.

Medical emergencies: The transfer is necessary for a medical emergency.

Staff authorising transfers of personal data outside the EU are responsible for ensuring that one of the above requirements is met and ensuring that a record is kept of which safeguard is in place.

For more advice on transfers of personal data outside the EU please consult the guidance: International Transfer Guidance

You can also contact the Data Protection Officer (DPO) dpo@activatelearning.ac.uk

11. Data Subject Rights

The UK GDPR lists eight data subject rights that the College will need to comply with, these are the rights of the data subject to:

- Be informed
- Subject access
- Erasure (to be forgotten)
- Rectification
- Portability
- Object
- Restrict processing
- Object to automated processing and profiling

Right to be informed: The right to be informed is complied with by issuing a privacy notice, please see Section 5.

Subject access right: The purpose of subject access rights is to allow individuals to obtain a copy of their own personal data, confirm the accuracy of personal data and check the lawfulness of

processing to allow them to exercise rights of correction or objection if necessary. The College must respond to all requests for personal information within one month. Any member of staff receiving a request from an individual for their own personal information should consult the relevant guidance: Dealing with Subject Access Requests

Right to erasure (to be forgotten): Data subjects have the right to request that their personal data be removed from all the systems of the College if certain requirements are met. These requirements are:

- The College does not need to keep the data anymore in relation to the purpose for which they were originally collected/processed.
- The data subject withdraws consent for the processing to which they previously agreed
- The subject uses their right to object to the data processing (possible where the legal basis is either 'public task' or 'legitimate interest').
- The College is processing the data unlawfully (i.e., in breach of the UK GDPR and/or the DPA)
- The personal data must be erased to comply with a legal obligation.
- The data subject was a child at the time of collection.

This means that if the legal basis for processing the data is 'performance of a contract' or 'legal obligation,' and processing is fully lawful, the request must be refused.

However, even if the request meets one or more of these requirements, there are still several exemptions when the College will not have to comply. Thus, data might not have to be erased if any of the following apply:

- The personal data is processed to exercise the right of freedom and expression (e.g., journalism, artistic work)
- The personal data is needed for legal compliance
- There are reasons of public interest around public health
- The data is processed and stored for scientific, historical research or archiving purposes in the public interest
- The data is needed for a lawsuit

Right to rectification: Data subjects are entitled to request that their personal data are rectified if the data are inaccurate or incomplete. If you receive such a request, you must comply within one month. Should complying with the request for rectification be particularly complex, then the time can be extended to two months.

If you have shared the personal data with third parties, or within the College, you must contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort.

Right to portability: The right to data portability gives data subjects the possibility to request that the College pass their personal data on to a third party of their choice and allow that third party to import the data automatically.

Data subjects have this right if certain requirements are met. These requirements are:

- The individual has provided the personal data to the College, and
- The legal basis for processing is 'consent' or 'performance of a contract,' and
- The processing is carried out solely by automated means with no human involvement.

If these requirements are met, then the data must be provided in a structured, commonly used, and machine-readable form.

Right to object: Data subjects have the right to object to the College processing their personal data if certain requirements are met. These requirements are:

- The legal basis for processing is 'legitimate interest' or 'public task;'
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

When data subjects have an objection on 'grounds relating to his or her particular situation,' then you must stop processing the personal data unless:

- You can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the data subject; or
- The processing is for the establishment, exercise, or defence of legal claims.

The right to object to profiling for direct marketing is an absolute right. That means that for such objections, data subjects will not need to provide any grounds relating to their situation, and the College is not allowed to override the objection.

Right to restrict processing: Data subjects have a right to 'block' or suppress processing of their personal data, i.e., to request that you immediately stop processing their personal data in any way except to store it. This right applies only if one of these requirements are met:

- A data subject contests the accuracy of the personal data - you should restrict processing until you have verified the accuracy.
- A data subject has objected to the processing (see above), and you are considering whether the College's legitimate grounds override those of the data subject.
- Processing is unlawful, the data subject does not trigger the right to be forgotten, but requests restriction of use instead.
- You no longer need the personal data and would delete them in accordance with the retention schedule, but the data subject requires the data for a lawsuit.

If you receive a request for erasure, rectification, portability, restriction, or an objection to processing, immediately contact Data Protection Officer.

Right to object to automated processing and profiling:

The prohibition

There is a clear prohibition regarding decisions based solely on automated decision making and on profiling which produce legal effects, or which similarly significantly affect an individual.

"Legal effects" have an impact on a data subject's legal rights, affect a data subject's legal status or their rights under a contract.

"Similarly, significantly affects" means the processing must be more than trivial and must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to significantly influence the circumstances, behaviour or choices of the data subjects concerned. At its most extreme, the decision may lead to the exclusion or discrimination of data subjects.

There are three exceptions from that prohibition, and that is where automated decision-making:

- is necessary for the performance of or entering into a contract;
- is authorised by law; or
- is based on the data subject's explicit consent

Data subject rights

Even where the three exceptions apply and automated decision-making and profiling can be used, data subjects still have rights. They can still object to the automated processing and request that a human being become involved and reconsider the decision.

Also, data subjects have the absolute right to object to profiling, as seen above under 'the right to object.'

If you believe that you are using automated processing or profiling, contact the DPO at dpo@activatelearning.ac.uk

12. Research

Research is governed by data protection legislation if it contains personal data or pseudonymised data. Data are personal if a piece of information directly identifies individuals or, if viewed in combination with other bits of information you have access to (or that you know), you could identify individuals.

Data are pseudonymised if you remove all direct identifiers from the research dataset, attribute a study specific identifier to each individual, and keep a link between both.

A dataset is truly anonymous when you can no longer identify an individual directly from the information combined with information that is available by other means or from other sources. This involves consideration of all the means likely to be used to identify an individual without going to significant effort.

Research under the UK GDPR will require informed, voluntary ethics consent to participate in a study, as well as a Participant Information Sheet.

The legal basis for processing personal data will be 'public task' and for special categories of personal data, 'necessary for scientific or historical research purposes in accordance with safeguards. These safeguards are what is currently considered good practice:

- The minimisation principle – use only the absolute minimum of personal data required for your purpose
- Anonymise personal data if you can
- If you cannot anonymise, wherever possible, pseudonymise all personal data
- Store the data securely

Furthermore, you must be able to prove that research is in the public interest. Evidence includes one of the following:

Your research must be proportionate e.g., it must not be more intrusive into participants' privacy than necessary, you must not collect more data than you need for your study

- Your research is subject to a policy research governance framework, e.g., the UK Policy Framework for Health and Social Care Research
- Research Ethics Committee (REC) review (does not have to be a European REC)
- Peer review from a research council
- In the case of medical research, Confidentiality Advisory Group (CAG) recommendation for support in England and Wales or support by the Public Benefit and Privacy Panel for Health and Social Care in Scotland.

When you have the necessary safeguards in place, the rights of research participants can be restricted. It will be up to the individual Principal Investigator's discretion whether the following rights should not apply where it would prevent or seriously impair the achievement of the research purpose and where your legal basis is public interest plus the additional research-related legal basis for special categories:

- The right to rectification
- The right to restrict processing
- The right to object to processing
- The right to erasure (right to be forgotten)

If your research involves collaboration with an industry partner, your legal basis will be 'legitimate interest.'

13. Student Research

Students may conduct research as part of their undergraduate work (dissertation) or as part of their postgraduate work (dissertations for a master's degree or a Doctorate). Students will remain the data controller and as such responsible for their research until they submit their dissertation. However, as students work strictly on behalf of themselves to achieve a degree, this processing activity falls under what used to be called the domestic uses exemption, which means that data protection legislation does not directly apply. However, students will be bound by the College's policy and procedures due to the Student Contract with the College.

Thus, the Data Protection Policy applies to students processing personal data as part of their work to pursue a course of study and they will be required to ensure that their work is compliant. They will also be required to conduct a data protection impact assessment as part of your Ethics Approval.

Once the dissertation is submitted, the College becomes a joint data controller with the student.

The only exception to this is where a student processes personal data whilst working on a project led by the College research group. In this case, the student and the College are both data controllers from the outset. More details can be found here: Personal data processed by students

14. Automated Decision-Making

Exam marking: The College does not use solely automated decision-making when marking exams. Even multiple-choice tests that may be checked and marked by automated means do not fall under the definition of solely automated decision-making, as the exam has been set by a human being, the correct answer has been determined by a human being and the automation applies only to checking the given answers against the correct one.

Learning analytics: When using learning analytics, the College will take the following approach as regards the legal basis:

- Use legitimate interests as the legal basis for the processing of non-sensitive personal data for analytics
- Obtain consent for processing of special category data
- Obtain consent to make interventions directly with students based on the analytics.

In accordance with the rights set out above under section 11, individuals can object to the processing where legitimate interest is the legal basis. For the situations where consent is required, that consent can either be withheld or withdrawn at any time.

15. Data Protection by Design and Default

Data protection by design (also called 'privacy by design') is an approach to projects and initiatives involving personal data that is intended to incorporate data protection compliance from the start, rather than considering it as an after-thought.

Thus, the College is required to implement the appropriate technical and organisational measures both at the time when the methods and ways of processing personal data are determined and at

the time of the processing itself. In addition, the College will need to ensure that, by default, only personal data that are necessary for each specific purpose are processed.

Examples for technical and organisational measures are:

- Data minimisation
- Additional layers of encryption
- Data retention limits
- Restricted access
- Anonymization and pseudonymisation
- Encryption, hashing, salting

All staff and agents of the College are required to apply the data protection by design principles when developing a new project or reviewing existing projects that involves the use or storage of personal data. The guidelines below explain the types of projects when this might be relevant, what data protection by design is and what measures can be put in please to protect personal data.

Data Protection Impact Assessments: One important measure that is expressly listed in the UK GDPR as a mandatory requirement is conducting a Data Protection Impact Assessment (DPIA) for projects or initiatives that may have a negative impact on data subjects' privacy. A DPIA is a type of risk assessment whereby potential privacy issues and risks are identified and examined from the perspective of all stakeholders.

A DPIA should be done as part of the initial phase of a project to ensure that risks are identified and considered before the problems become embedded in the design and causes higher costs due to making changes at a later stage. Also, if there is a change to the risk of processing for an existing project a review should be carried out.

The DPIA will then continue to assess privacy impacts throughout the lifespan of the project. Examples of the types of projects where a DPIA needs to be considered include:

- Building or buying new software or IT systems for storing or accessing personal data
- Developing policies or strategies that have privacy implications
- Embarking on a data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A new surveillance system such as CCTV
- Using personal data for new purposes such as a new database which consolidates information held by separate unrelated parts of the College.

In addition to meeting legal requirements, taking a proactive approach to privacy will reduce the likelihood of fines or financial losses due to data protection breaches and help build reputation and stakeholder confidence.

Guidance on how to conduct a DPIA can be found here: Data Protection Impact Assessment and Guidance

Pseudonymisation: Pseudonymisation is a privacy-enhancing technique; it is a process rendering data neither completely anonymous nor directly identifying. With pseudonymisation you separate personal data from direct identifiers so that linkage to an identity is no longer possible without the additional information that is held separately. It is important to note that pseudonymised data is not exempt from the UK GDPR and the DPA.

If you pseudonymise a research dataset by keeping the data and the identifiers separate and send the pseudonymised data to another College without also sending the identifiers, then the other

College will process anonymised data as the UK applies a concept of relative anonymity. You, however, will still process personal data as you can still at any time re-identify individuals. In countries such as Belgium, the other College would still process personal data as the key exists somewhere in the world – Belgium applies a concept of absolute anonymity.

Under certain circumstances, pseudonymised data can be exempt from data subject rights. This exemption, however, applies only if you can demonstrate that you are not able to identify the data subject anymore, e.g., when you destroy the identifiers, but you know that they still exist elsewhere. You will then not be required to comply with subject access requests, as the UK GDPR does not require a controller to hold additional information for the sole purpose of complying with such requests. If, however, data subjects provide you with the additional information you would require to re-identify them in the data set, they must be permitted to exercise their rights.

Anonymisation: Anonymised data means that all identifiers have been irreversibly removed from data subjects and they are no longer identifiable in any way. In this case, the UK GDPR and the DPA do not apply any longer – the data is no longer personal. However, with the advances in modern technology, re-identification will become easier. The ICO applies the concept of the 'motivated intruder': data will be considered anonymous unless an individual has the motivation to spend a considerable amount of time, effort and/or resources to re-identify people.

16. Direct Marketing

Direct marketing includes the advertising or marketing of commercial products or service, as well as fundraising, and includes all messages promoting an organisation. Such as promoting College events or opportunities for students.

Direct marketing covers all forms of communication, such as marketing by letter, telephone, email, and other forms of electronic messages.

Finding the correct legal basis for direct marketing is particularly important. The law distinguishes between direct marketing using electronic means and non-electronic means. Currently, 'electronic means' covers the use of email and text messaging. For marketing by letter and telephone (unless the individual is registered with the Telephone Preference Service), the UK GDPR applies, and your legal basis can be 'legitimate interest' – you will not need consent.

The Privacy and Electronic Communications Regulations 2003 (PECR) regulate the use of electronic communications such as email or text messaging as a form of marketing.

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts, and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Electronic marketing to private individuals can only be done with consent as the legal basis. Consent must be 'opt-in' and any direct marketing messages should only be sent to those people who have in fact opted in. One exception to the need to obtain prior consent is the so-called 'soft opt-in,' which is based on 'legitimate interest.' Soft opt-in can be used in situations where you have a pre-existing commercial relationship with the individual, if you provide the option to 'opt out'

(unsubscribe) in every email and inform people when you collect their data that there will be marketing and that they can opt out.

The full guidance on direct marketing can be found here: Direct Marketing under Data Protection Law

17. Data Protection Breaches

A data protection breach is defined in UK GDPR to mean:

> "a breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

The UK GDPR imposes a requirement that certain data protection breaches be reported to the Information Commissioner's Office within 72 hours of the College becoming aware of the breach.

While the College makes every effort to avoid data protection breaches, it is possible that mistakes will occur on occasions or things will happen that are beyond the College's control. This section of the Handbook sets out the procedures to follow if a personal data incident has occurred. All individuals who access, use, or manage the College's information are responsible for following these guidelines and for reporting any data protection incidents that come to their attention.

A personal data incident can occur for several reasons some examples of these include:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g., email sent to incorrect recipient or document posted to the wrong address or personal information posted onto the website without consent)
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

Reporting an incident

It is the responsibility of any staff, student or other individual who discovers a personal data incident to report it immediately to the DPO at dpo@activatelearning.ac.uk with 'data incident – potential breach' in the subject line. You will then have to fill in a Data Incident – Potential Breach Form, which can be found here: Data Incident – Potential Breach Form

The DPO will require information from you about the nature of the incident / potential breach, i.e., what happened, and whether any personal data was involved. This could be the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The DPO, through investigation, will determine whether the incident constitutes an actual data protection breach and will act accordingly to help contain the incident and, where necessary, assist with notifying the affected data subjects. The DPO will also, if required to, report the matter to the ICO, notify the COO (Chief Operations Officer), Senior Executive Assistant, Head of Governance, and the Information Commissioner's Office.

The DPO will keep a record of all data protection incidents and breaches including the actions taken to mitigate the breach and the lessons learnt.

18. Emails and Mailing lists

Privacy notices: Whether your communication is internal or external, electronic or in paper format, you must always ensure that recipients receive a privacy notice, through either a link or the entire privacy notice in the footer of all emails, and a link or the entire privacy notice included in all letters sent out.

External mailing lists in paper format: If your external mailing list is used to send communications in paper format, you will not need to obtain consent. Instead, your legal basis is 'legitimate interest.' You must, however, provide recipients with the opportunity to easily and effortlessly, opt out of receiving the communication in every letter.

External mailing lists in electronic format: ***Business-to-business (B2B).*** If you send emails to business contacts, i.e., individuals who can be considered as representatives of their company, organisation, or institution (e.g., students or academics from another College), you can rely on legitimate interest. However, you must first provide a privacy notice and then the option to opt out in every communication.

Private individuals. If you send emails to private individuals, then you must have obtained consent. If an existing mailing list contains exclusively or mostly private individuals who have not subscribed but have been added to the list, then you must request consent and remove those who do not reply from the list. After an appropriate period, consent must be refreshed. Always provide first a privacy notice and then the option to opt out in every communication.

Mixed lists. If your mailing list contains both B2B contacts and private individuals and you have not obtained consent from the private individuals, conduct a risk assessment to determine whether continuing to send emails is likely to cause offence or distress or whether receiving the emails is in the individuals' interest and/or to their benefit.

Email service provider. The College uses Mailchimp for email marketing lists. For further details, contact the Head of Marketing.

Internal mailing lists in electronic format: For essential business mailing lists with information such as changes in lecture theatre for students, information about lack of heating or power failure in certain buildings, subscription is mandatory and an option to unsubscribe cannot be given and the legal basis for these emails is 'contractual obligation.'

For non-essential mailing lists about, for example, events on a campus or career opportunities for students, staff members and students are business contacts, and the legal basis for these emails is 'legitimate interest.' Always provide the option to opt out in every communication.

Mailing list service: For internal mailing lists using Outlook and Mailchimp, the full guidance on mailing lists can be found here: Mailing lists and data protection

19. CCTV

For CCTV systems, two types must be distinguished:

- Cameras that record
- Cameras that only show live footage but do not record

Only cameras that record fall under the UK GDPR and the Act.

However, even if cameras that only show live footage are not subject to the UK GDPR and the Act, it is good practice to include them when complying with the fairness and transparency requirements, i.e., when displaying appropriate signage where cameras are in use.

Only for cameras that record, are you required to have a legal basis. This legal basis depends on the purpose for the cameras.

- If the cameras are in a high-security laboratory, you will be able to rely on 'legal obligation.'
- In all other locations, your legal basis will be 'necessary for legitimate interest,' as the cameras will be intended to assist with general safety and security.

Individuals whose images are recorded have a right to view the images of themselves and to be provided with a copy of the images.

Further guidance can be found in the CCTV policy: CCTV Policy

20. Photography

Whenever individuals can be identified by their image, data protection legislation applies. In these situations, the rights of the individuals in the collection and use of their photographs must be respected – they must be informed when an identifiable image of them will be or has been captured, and a legal basis must be found before the image is used in any way.

Photographs of individuals and posed groups: When taking photographs of a specific person that you might want to publish on the internet, you can use 'legitimate interest,' 'consent' and 'contractual obligation' as your legal basis. Remember that consent can be withdrawn at any time, and you will have to react accordingly.

Photographs of crowds: If crowd shots are taken during an event and an individual is not identifiable, then it is not necessary to have a legal basis to take, display or publish the photo. This applies to any individuals, students, and staff whose images are incidental detail, such as in crowd scenes for graduation, conferences and in general campus scenes. If the photos are taken at a conference where it is likely that individuals may be identified even in crowd scenes, then your legal basis is 'legitimate interest.'

You must, however, include notices at the event informing attendees of the fact that photos are being taken so they can opt out.

Photographs of children: If taking photographs of children, you must obtain consent from a parent or guardian. This may be written or verbal depending on the circumstances, see the guidance above.

The full guidance on photography can be found here: Photography guidance

Definitions

1. Personal Data.

Data protection legislation applies only to personal data about a living, identifiable individual.

Personal data is data about a living individual. That living individual must be identifiable, either directly or indirectly, usually through a so-called identifier (such as name, identification number, GPS location data or online identifiers such as a computer IP address).

- Directly identifiable

Directly identifiable means identifiable from the information itself, for example, a name together with an address, age, telephone number.

- Indirectly identifiable

Indirectly identifiable means not identifiable from the information itself, but from the information combined with data from another easily available source.

Example 1:

Recorded research interviews together with entries in a database linking voice recordings to names; or a student number together with the research entry linking the number to the student.

Example 2:

You remove the identifiers from a research dataset and store them separately. This leaves you with so-called pseudonymised data, which is still personal data as you can re-link the data and the identifier at any time, enabling you to re-identify individuals.

Important for determining whether individuals are indirectly identifiable is content, context and whether a 'motivated intruder' would be willing to spend the time, effort, and expense to attempt to identify somebody.

Example 1:

You take a photo for a brochure showing students relaxing in George Square gardens. Without your knowledge, the daughter of a celebrity is in the photo with her new boyfriend. A journalist spotting the picture and attempting to identify the boyfriend would be considered a 'motivated intruder' – somebody who is willing to make the effort to identify somebody.

Example 2:

You pseudonymise a dataset and send the de-identified data without the identifiers and the key to a college in London. The London college will receive anonymous data as no researcher there would be interested in making the effort to re-identify individuals, they are only interested in conducting their research.

The personal data must be held by the College either electronically or in paper format in a 'relevant filing system.'

1.1. Special categories of personal data

Some personal data comes under the heading of special categories of personal data. This type of data is subject to further regulations under current data protection legislation and can only be processed under certain circumstances. Refer to the guidance in Appendix 5

2. Data subject

A data subject is an individual who is the subject of personal data. *For example, we hold personal data about students, making each student a data subject under the terms of the legislation.*

3. Data processing

Data processing includes reading, amending, storing, and deleting data. Data processing is any action taken with personal data. This includes the collection, use, disclosure, destruction and holding of personal data, even its anonymisation.

4. Data controller

A data controller is an organisation that has full authority to decide how and why personal data is to be processed, and that has the overall responsibility for the data. This includes deciding on use, storage, and deletion of the data.

The College as data controller:

When the College decides that it wishes to share the personal data it holds with another organisation we are acting as a data controller, as we have the authority to take this decision.

Receiving organisation as data controller

The receiving organisation may also become a data controller. This will depend on whether it will have the authority to decide how and why the data will be stored, used, and deleted. If the receiving organisation has considerable discretion in this area, it is a data controller.

Example

Passing information, such as the destinations of leavers, to ESFA or schools for analysis is done as a data controller-to-data controller transfer. This is because the ESFA or the school is a separate organisation and will be using the data for their own purposes, which the College will not be involved in or have control over.

If the College were to retain control, this would be a data controller-to-data processor transfer.

5. Data processor

A data processor is an organisation that processes personal data on behalf of another organisation

If the College passes personal data to an organisation to carry out the College's work on the College's behalf and instructs this organisation on what should be done with that data and how to do this by means of a contract, then the receiving organisation is a data processor. The College will only be legally responsible for any breaches of data protection legislation by a data processor if no contract is in place, and if the College has not satisfied itself that the data processor has adequate security provisions in place.

Example

If information held in the College library database is passed to an information technology company to carry out maintenance tests, this is done so as a data controller-to-data processor transfer. This is because the College will retain control over the data and the purposes for which it is processed.

If the College were not to retain control, this would be a data controller-to-data controller transfer.

6. Sentry

Sentry is the College's online data protection management system. Sentry holds the registers for Data Breaches, FOI's, Rights Requests, etc. It also maintains the retention register and Register of Processing Activities (ROPA).

Privacy notices

This guidance is for any member of the College staff who needs to make sure they have a compliant privacy notice. Please note: The names 'privacy notice' and 'privacy statement' are used interchangeably.

Check existing privacy notices

Consider whether the information you wish to convey is already detailed in one of the College's existing corporate privacy notices. If so, provide a link to the relevant privacy notice when communicating to a data subject how their personal data will be processed.

- Privacy notices for students
- Privacy notices for employees
- Privacy notices for systems and processes

Templates for privacy notices

Prior to producing a Privacy Notice, please check first with the Data Protection Officer whether the activity for which you require a privacy notice is already included in the corporate Privacy Notice.

For situations where this is not the case and for all other processing, we have designated templates for some of the most frequent functions that involve the processing of personal data. Adapt these templates as appropriate to make them suitable for your data processing activity.

Note that when someone sends you information of their own accord or makes an enquiry which contains their personal data, you will not need to provide them with a privacy notice. You should, however, delete the information when you no longer need it.

The corporate Privacy Notice can be found here: Privacy and Data Protection – Privacy Notice

If you need a privacy notice for a different purpose than those shown in the above link, contact the DPO who will provide you with a generic privacy notice template to customise. The privacy notice comes in two parts. Customise the template (which comprises of five sections) and make it available to your data subjects. Guidance on how to customise a privacy notice is provided in Appendix 5 Guidance on Legal Basis for Processing.

Generative Artificial Intelligence

Guidance for staff and students on the processing of personal data using Generative Artificial Intelligence (such as ChatGPT)

Generative Artificial Intelligence stores and learns from data inputted, however AI systems are required by **data protection law** to process personal data fairly and lawfully. It is not currently always possible to delete data from an LLM (large language model tools) neural net. Therefore, these systems may not be complaint with relevant law like the UK GDPR and the Data Protection Act.

To ensure the privacy of individuals, personal and sensitive data should not be entered into generative AI (Artificial Intelligence) tools. Any data entered should not be personally identifiable and would be considered released to the internet.

If staff and students nevertheless decide to introduce new AI systems and tools for processing personal information, then they must undertake a Data Protection Impact Assessment (DPIA) to determine the privacy risks and if those can be mitigated. They must consider if there are less risky alternatives that can achieve the same purpose and must adequately justify their decision not to choose them.

For further information, please see the College guidance and advice on the use of Artificial Intelligence. AI and Activate Learning – Position Statement

Sharing personal data

These webpages explain how College staff should deal with non-routine enquiries to share information about third parties

The College should not disclose information to a third party without a good reason. There are some circumstances where sharing is appropriate.

This guidance explains

- when you can share personal data
- when you need to refer an enquiry to the correct decision maker or department
- when you should refuse to disclose information.

If you need to share personal data with another data controller, please contact the DPO at dpo@activatelearning.ac.uk

If you receive a data subject access request or a request for data portability, please contact DPO at dpo@activatelearning.ac.uk

1. When to Share

1.1. Emergencies. Sharing information in an emergency to prevent injury or damage to the health of a person

You can share personal information where disclosure is urgently required to prevent injury or damage to the health of any person.

Where possible, get permission from the individual before sharing information with a third party. Otherwise, share the information only if it is a matter of life or death.

Compassionate disclosure

It can be appropriate to share information in response to requests of a compassionate nature (such as attempts to find out a student's whereabouts in the event of a family bereavement). However, the relevant head of department or director of faculty must authorise sharing the information.

If it is not appropriate to pass on confirmation of a student's whereabouts, or confirm they are a student, you can offer to pass on a message on a conditional basis.

Passing on a message

If a third party wants to contact a student, where appropriate, you should offer to forward a message to the student with details of the enquiry, so the student can decide for themselves whether to contact the third party. Do this without saying whether an individual is or is not a student.

For example, this is an appropriate way to respond to an enquiry from a friend or family member of a student who has lost touch with someone they believe to be a college student.

Contacting the student

If the enquirer confirms they would like us to pass on a message, and the College has contact details for the student, pass the message on to the student.

Sharing with consent

You should ask a student for consent to share information about them, where:

- you would not share the information without consent if the student refuses
- you believe that it may be in the student's best interest, or the student may wish the College to share the information in the circumstances

Alternative: forward a message to the student

Consider whether it is simpler to pass on a message to the student, so the student can decide for themselves whether to share information direct with the enquirer.

If the student has asked you to share personal information about them with a third party, this would also be sharing information with consent. You must still make sure the criteria below are met.

1.1.1. Criteria

You must ensure that consent is freely given, specific and informed. This means you must:

- be clear exactly what information will be shared.
- provide the student with enough information to help them to make an informed decision.
- be clear to the student that sharing of information is optional.
- not pressurise a student one way or the other

1.1.2. Record keeping

You must

- keep a record of the consent gained.

How you do this depends on the risk involved. If the information shared is sensitive, for example information about the student's health or mental wellbeing you should usually ensure you have the information in a recorded format where you have verified is from the student.

1.1.3. Further guidance

More detailed guidance on consent.

2. When to Refer

Staff should refer decisions about sharing personal data to the relevant senior decision maker or department responsible for the information.

2.1. Police enquiries, and similar agencies

Guidance for staff who receive an enquiry from the police or other agency requesting the College shares personal data about a student or staff member.

The Police or other agencies such as the Department for Work and Pensions (DWP (Department for Work and Pensions)) or HMRC may contact staff with requests to share information about identifiable living individuals.

Staff members should:

- Not confirm or deny any information about any individual student on the spot.
- Confirm the enquirer is who they say they are. Be aware there are people who will try to "blag" personal information about individuals.
- Ask for the enquiry to be provided to the College in writing. If the enquiry comes from the Police, they should provide a form citing Data Protection Act 2018 – Schedule 2, Part 1(2) counter signed by a senior officer. Please note, however, that this only applies while the investigation is still ongoing. If the police ask for somebody's personal data with a warrant for an arrest and show you the required paperwork, then you must comply.
- In all situations, if the Police have no counter-signed Schedule 2, Part 1(2) form and cannot provide evidence for the urgency of the situation, then you should not comply with their request.
- Direct the request to the relevant Director or Head of Department responsible for the requested information.

2.1.1 Responsibilities for student data

These are the key staff who are responsible for decision making

Type of information	Director / HoD responsible
Student or staff use of College computing equipment or login details	Director of IT Services / Group IT Systems and Infrastructure Manager
Student or staff library use / borrowing history / library fines	Group Director of Digital Education / Group Learning Environments Manager
Student's status / centrally held academic records	Group Director Institutional Effectiveness / Group Data Manager
Datasets about groups of students	Group Director Institutional Effectiveness / Group Data Manager
Information held only by the student's faculty	Delivery Director / Faculty Manager
Student's Counselling service use	Director of Safeguarding

The Director or Head of Department must:

- decide whether to disclose the information
- consider whether the student or staff member should be told about disclosure
- make sure the request is answered in an appropriate way

Guidance for decision makers is available from Data Protection Officer who may involve Legal Services where appropriate.

2.2. Fraud or Misrepresentation

What to do when you receive an allegation of fraud or misrepresentation

It is appropriate to share personal information in the interest of protecting individuals, employers, and the College from fraud and/or potential fraud. For example, if an individual says they have a degree from the College and they do not, the College can ask them to stop making the claim and confirm they do not have a degree.

However, the appropriate Director or Head of Department must decide on the best course of action.

2.2.1. Assessment and Awards results

Concerns about fraud or misrepresentation of college awards and results or student status must be forwarded to the Exams Team of the appropriate College campus

2.2.2. Employment

When anyone is deemed to have the potential to bring the College into disrepute or has brought the College into disrepute by claiming, through the use of any media, to have been employed by the College in any capacity which we cannot validate, concerns should be forwarded to the Human Resources team.

Contact the DPO for advice on data protection aspects of disclosure.

However, if there are wider legal issues involved in the disclosure, you should also contact Governance for access to the College Legal Services.

2.3. Degree verification

Guidance for staff on receiving requests to verify awards

Requests from employers, recruitment agencies or educational institutions to verify awards of students should be referred to the Exams Team of the appropriate College campus.

2.4. Visas and immigration

Requests to share information about students relating to visas and immigration

Requests to share information about students in relation to visas or their immigration status, for example from the UKVI, must be referred to the Group Administration team.

2.5. Media enquiries

How to deal with a media enquiry about a member of College staff or a student

If you receive an enquiry from a journalist about a student or staff member, pass the enquiry to the Communications and PR Team without comment.

The Communications and PR Team will identify the relevant senior decision maker and liaise with them to respond.

2.6. Court orders

Guidance for staff who receive a court order to share personal information

Court orders should be passed to Governance for forwarding to the College Legal Services immediately.

The department responsible for the information requested remains responsible for compiling and providing the requested information.

2.7. Large scale disclosures

How to deal with requests for large scale disclosure of personal data

Requests for large scale disclosures of personal data of multiple individuals should be considered as transfers of personal information.

If information comes from a core College system, disclosure should be approved by the relevant Director or Head of Department following a discussion with the DPO.

3. Refusing to disclose

If you have received a request for information about an individual in recorded format (e.g., in writing), and are refusing the request, you should record the matter and inform your manager of the decision.

3.1. Parents and family members

Guidance for staff who receive a request from family members to share personal data

Parents and family members of students and staff have no general legal right to be given information about those individuals.

Do not share information or discuss issues with parents or family members of students.

Sharing by request

If a student has asked you to share information with their parent or family member, you can do so, provided you ensure you have specific, freely given and informed consent from the student.

Guidance on seeking consent

General information

You can share general information about College policies and procedures with a parent, where this sort of information would be shared without hesitation in response to a freedom of information request.

For example, if a parent wants to know about their son's options for suspending his studies, you can send the parent a link to the relevant College procedure. However, do not discuss anything specific about the son's circumstances.

Passing on a message

If a family member is unable to contact a student, you can offer to pass on a message, and explain it is the student's decision whether to respond. You should not confirm or deny someone is a student when doing so.

Passing a message guidance and model text

Emergency contacts

If there is an emergency, for example a student is rushed to hospital, you can contact their listed emergency contacts to let them know about the situation. However, do not share additional information about the student that is not relevant to the emergency.

Exceptional circumstances

If there are exceptional circumstances, where you think it may be appropriate to share information, you should refer the enquiry to the relevant senior decision maker.

Guidance on Legal Basis for Processing

How to determine the legal basis for processing personal data.

This guidance is for any member of College staff tasked with determining the legal basis for processing personal data to ensure that all data processing is lawful.

You will need to use this guidance:

- When customising a privacy notice to ensure it complies with current data protection legislation
- When conducting a 'data protection impact assessment' (DPIA)
- When otherwise collecting or receiving personal data for a new initiative

The legal basis:

Whenever we use personal data, we must have a legal basis for doing so.

Data protection legislation gives us a list of possible legal basis we can choose from.

If you are using special categories of (sensitive) personal data, there are additional legal basis you must comply with. See the guidance on special categories.

1. Consent

How and when to use consent as the legal basis for processing personal data

Use this guidance when intending to use personal data and none of the other legal bases (such as contractual obligation or performing a task in the public interest) are applicable.

The basic rules of consent

The requirements for consent are stringent to protect the rights of data subjects. Consent must be:

- Freely given
- Specific and informed
- Active opt-in
- Verifiable
- Withdrawable

Consent is inappropriate if data subjects do not have a genuine choice over how data about them are being used. This would be the case if you would still process the data under a different legal basis if consent were refused or withdrawn. In these circumstances consent would be misleading and inherently unfair.

1.1. Marketing

If you are carrying out marketing activities, you must also follow the guidance on marketing as additional legislation applies.

Marketing does not only include the offer for sale of goods or services, but also the promotion of an organisation's aims and ideals. For example, a 'healthy lifestyle' promotion, or a promotion of the College's cafeterias with a free coffee for the first 20 students presenting a coupon.

1.2. Active opt-in

Under data protection legislation, consent must be an unambiguous indication, which means that consent must be either a statement or an affirmative action. Consent must be more than just confirmation that the person has read terms and conditions – there must be a clear signal that they agree.

Clear affirmative action means someone must take deliberate action to opt in.

This could be through

- ticking an opt-in box

- signing a consent statement
- oral communication
- a binary choice presented with equal prominence
- switching technical settings away from the default.

The key point is that all consent must be opt-in – there is no such thing as 'opt-out consent.' Failure to opt out is not consent and you may not rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions.

Implied consent, however, is still possible in circumstances where the individual has shown consent through an action. Again, mere silence or inactivity are insufficient.

For special categories of sensitive personal data, consent must always be in writing.

Example:

"Would all those who want to be in the conference photo please make their way onto the stage. We will publish the photo on the conference website."

This would suffice for consent as conference participants have shown their consent through an action, i.e., going onto the stage.

At recruitment fairs or the College Open Day, potential applicants consent to receiving information material by providing their email address.

1.3. Freely given

Freely given consent means that people have a genuine choice and control over how the data controller uses their data. This means that the data subject must be able to refuse to give consent without any detriment and must be able to withdraw consent easily at any time. There must be no imbalance in the relationship between data controller and data subject. Consent must not be a prerequisite for provision of a service.

1.4. Imbalance of power

Consent will be inappropriate if there is a clear imbalance of power between data controller and data subject. This is because consent cannot be freely given if data subjects feel they have no choice but to agree to the data processing. For example, data subjects may depend on a service or fear adverse consequences if they do not consent.

1.5. Condition of service

If a data controller arranges for a service to be dependent on the data subject consenting to data processing, then consent will not be valid as it will not be freely given. However, providing incentives such as loyalty schemes, is possible.

For example, staff and students may be persuaded to sign up to a cashless catering system and as a reward for allowing the company to send them special offers, they will receive vouchers and a free cup of coffee on their birthday.

Examples of inappropriate consent

A lecturer asks students for consent to have their photos and contact details displayed on a public website linked to a project and says otherwise they will not be able to participate in the project.

The HR department asks potential employees for their consent to have their dates of birth, salary and private addresses transferred to the cashless catering system as otherwise they will not be able to participate.

1.6. Specific and informed

For consent to be specific and informed, people must first be aware of the identity of who is processing their personal data. Both the College and any third-party data controllers relying on the consent you are aiming to obtain will need to be expressly named. It is not enough to simply define a category of third parties.

Examples

*This consent request would **not** be sufficient:*

"You agree to the College, and any recruitment agencies with whom we might consult, processing your personal data in order to help you with your career choice."

This consent would be sufficient:

"You agree for the College to transfer your data to the College's Careers team to help you with your career choice."

People must also know what it is they consent to. This means that you must provide information in the relevant privacy notice about all the purposes for which personal data is being processed. Refer to the guidance about privacy notices. Privacy Notice

1.7. Verifiable

You must have an effective audit trail of how and when consent was given, so you can provide evidence if challenged, which means that you will need to keep a record in order to demonstrate what the person has consented to, including what information they were given, and when and in what way they consented.

You also need to record when people have withdrawn their consent. The consent record needs to be kept for as long as you continue to hold information about the data subject for that purpose.

1.8. Withdrawable

If you rely on consent as the legal basis for processing data subjects' personal data, they have the right to withdraw their consent at any time. Therefore, when you ask for consent, you should include details of how it can be withdrawn. Withdrawing consent must be as easy as giving it. There should be an easily accessible one-step process which people can use on their own initiative at any time. If possible, people should be able to withdraw their consent using the same method as they gave it. For example, provide an 'unsubscribe' link in every email or an email address, freephone telephone number or freepost address in your communications.

Once consent has been withdrawn, stop processing as soon as possible. However, if a person withdraws their consent, it does not retrospectively affect the processing already undertaken. For example, if somebody has consented to participate in research, they will not be able to ask you to remove data about them from studies which have already been published, but they can change their mind about raw data about them being used in future studies.

1.9. Unbundled

Consent requests must be clearly distinguishable from the rest of the text of the document or form you use; it needs to be separate from other terms and conditions and easily identifiable as a request for consent. Either use a separate consent form or ensure that the consent request is kept separate at the bottom of a form.

Example of 'bundled,' invalid consent

"We will collect your name, date of birth and any medical conditions from you. We will process the information you have provided us to enable you to use the College Sports Centre and take part in classes. You agree to us passing your personal data on to our sponsor who will send you marketing material for sportswear with the College's logo. We will also use the information you have provided us with to ensure you are kept informed of any new classes we offer. We will keep the information you have provided for as long as you are matriculated. We do not use automated decision-making or profiling.

Please sign here……."

1.10. Granular

Wherever appropriate, you will need to provide data subjects with granular options to consent separately to distinct types of processing. If you obtain consent for, say, processing personal data for displaying student photos on your website, you must have separate consent for using the photos

for newsletters or for marketing purposes. Only if the activities are clearly interdependent or if providing a granular list of consent would be disruptive or confusing can you provide a single option for consenting.

The most crucial factor is that you clearly explain to people what they consent to in an understandable way. Should your purposes for processing the personal data change, you will have to consider reconsenting people as there is no such thing as 'evolving' consent.

How long does consent last?

There is no specific time limit for consent. However, consent is likely to 'degrade' over time, but the exact duration will depend on the context. Both the scope of the original consent and the data subjects' expectations need to be considered.

Consent will need to be reviewed regularly to check the relationship, processing and purposes have not changed. Processes must be in place to refresh consent at appropriate intervals.

A record of when and how consent was received and of the information provided to data subjects at the time of consenting must be kept.

Should data subjects withdraw their consent, a suppression lists must be kept managing the withdrawal of consent and ensure that these data subjects are not contacted and/or asked for consent again.

If personal data has been received from third party data controllers, you will need to ensure that they have obtained consent from the data subjects before.

Examples

The College Hair & Beauty Salon runs a promotion that gives members the opportunity to opt in to receiving emails with tips about healthy living to get in shape for the summer holidays this year. As the consent request specifies a particular timescale and end point – the summer holiday – the expectation will be that no more emails will be sent out once the summer is over. The consent will then expire.

College Alumni can under the legal basis of legitimate interest contact individuals that are not alumni of the College and ask them to become donors. If an individual refuses consent to any further communication, then that individual's name and contact details must be entered into a suppression list to avoid any future contact.

2. Legal obligation

Processing personal data for any statutory or legal obligation imposed on the College is legitimate if the processing is necessary to comply with that obligation.

Example:

Sending staff data for tax purposes to HMRC or sending student data to the UKVI regarding visa applications.

3. Public tasks

Processing personal data based on public tasks. This legal basis will apply only where the task carried out, or the authority of the controller, is laid down in UK law. Thus, this is the legal basis to use for performing tasks with personal data that relate to the core functions (the reasons the College was established) of the College.

This legal basis covers data processing to perform tasks that are required to provide an education. For example, data processing related to:

- lecturing and tutoring
- marking exams
- awarding qualifications
- historic or scientific research

4. Special categories

Some personal data comes under the heading of special categories of personal data. This type of data is subject to further regulations under current data protection legislation and can only be processed under certain circumstances.

Personal data is classed as belonging to "special categories" under current data protection legislation if it includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- physical or mental health
- sexual life or sexual orientation commission of offences or alleged offences
- genetic data
- biometric data

The updated guidance from the Information Commissioner's Office for genetic data states:

“So, in practice, genetic analysis which includes enough genetic markers to be unique to an individual is personal data and special category genetic data, even if you have removed other names or identifiers. And any genetic test results which are linked to a specific biological sample are usually personal data, even if the results themselves are not unique to the individual, because the sample is by its nature specific to an individual and provides the link back to their specific genetic identity.”

The College interprets this as follows:

In certain cases, a single or few markers in genetic analysis will not be sufficient to make genetic data identifiable, if used in research without phenotypes or other identifiable data. This, however, will be a rare occurrence. In all other cases, genetic analysis will be considered identifiable and therefore personal data

Legal bases for processing special categories of personal data

a. Explicit consent of the data subject

To rely on explicit consent for special categories of personal data, the same basic requirements as those for consenting to the processing of regular personal data apply.

However, the requirements for explicit consent extend beyond that, which means that implied consent is not acceptable and the ‘clear affirmative actions’ that meet the requirements for ordinary consent are not sufficient. The key difference is that ‘explicit’ consent must be affirmed in a clear statement.

Explicit consent will be:

- A signature from the data subject
- A tick in an unchecked box by the data subject to say ‘I consent’
- An oral statement ‘Yes, I agree’

Even in written context, not all consent will be explicit.

Difference between implied and explicit consent

Example

The Student Support Service provides the following to students registering for the service:

"Email address (optional) - We will share your file with selected therapy centres and have them send you information to help you further."

Example

The Student Support Service provides the following to students registering for the service:

"I consent to you sharing my file with selected therapy centres and receive emails from them."

In Example 1, the students, while actively entering their email, still give implied rather than explicit consent. In Example 2, they are giving a clear statement by ticking the box.

If you intend to use explicit consent as your legal basis, see the guidance on consent.

b. Necessary for employment law or social security law purposes

This legal basis is likely to be used in a HR context where an employee's sensitive personal data might be used to, for example, to adapt a workstation.

Example

Changing an employee's contract to part-time after an illness.

c. Necessary to protect vital interests

This replicates broadly the legal basis for processing ordinary personal data – if a person is incapable of giving consent due to, for example, being unconsciousness, medical data can be provided to the paramedics.

d. Processing by not-for-profit bodies or associations

This condition does not apply to the College – it only applies to bodies or associations existing for political, philosophical, religious or trade union purposes.

e. Personal data manifestly made public

Sensitive personal data can, for example, be considered to have been made public by the data subject through a media interview published in a newspaper or broadcast on TV.

In the case of publishing through social media, this will need to be considered on a case-by-case basis. If you are in a situation where you may wish to rely on this legal basis, please contact the Data Protection Officer for advice.

This does not include photographs, even though they might show the racial group or even the sexual orientation of an individual. Neither does it include information that a data subject has announced to a gathering of friends.

f. Establishment, exercise, or defence of legal claims

This will cover most activities of lawyers acting on behalf of the College and carrying out the College's instructions.

Examples

HR processes an employee's sickness absence information with a view to seeking legal advice on an unfair dismissal allegation.

The College passes a student's information about the student's dyslexia on to the Legal Team as the student has threatened legal action, insisting that there was not enough extra time during an exam.

g. Substantial public interest

Additional legislation has been created to make the processing of special categories of personal data legal for the purposes of providing counselling services and to detect and investigate malpractice.

h. Medical purposes and the provision of health or social care

This legal basis will be used in situations where the processing is necessary for the purposes of occupational medicine and social care as well as preventative medicine and diagnosis, the provision of health care and treatment and the management of health or social care systems and services.

The data processing must be carried out by a professional who is subject to the duty of confidentiality, or a non-professional who is subject to the same standards.

This covers medical professionals in the College i.e., nurses.

i. Public health

This legal basis permits the processing sensitive personal data in cases of threats to health from infectious diseases. Should a case of, for example, Covid, cholera, or TB occur on a College campus, then the College and the NHS will have the legal duty to notify the government to prevent the spread of the disease.

j. Archive, statistical and research purposes

If possible, all personal data – both special categories and ordinary personal data – should be anonymised for archiving, research, and statistics. If that is not possible, then data protection legislation allows the activities to be carried out under suitable safeguards.

Examples

Archiving material from a conference held on Campus.

Conducting a longitudinal study which requires regular data from students' health records to be fed in. Complete anonymisation would not be possible.

Providing information to a Government Education Agency.

5. Performance of contract

When to use the legal basis that processing personal data is necessary for the performance of a contract. This legal basis will be used if:

- processing personal data is necessary for the performance of a contract
- or if requested by the data subject, for the preparatory steps to enter into a contract.

This request does not have to be expressly worded – if prospective students submit an application to the College, then their request to process the data is implied.

It is important to note that the only requirement is for the data subject to be party to the contract. This means that if a data controller only acts as a facilitator to enable a data subject to enter into a contract with a third party, then this legal basis is applicable.

Examples

HR evaluating a job applicant's personal data to decide whether to send a job offer will be 'steps taken at the request of the data subject prior to entering into a contract.'

Accommodation Services helping a student apply for a private flat to rent during the academic year even though they are not party to the contract.

6. Vital interests

Processing is necessary to protect life and death of an individual. Processing is necessary to protect the vital interests of the data subject or another natural person. Vital interests are only ever those relating to life and death issues. This legal basis will cover any emergency medical situation.

Example:

A student collapses during a lecture and is unconscious. The lecturer calls for an ambulance and gives the paramedics the student's name and address.

7. Legitimate interest

Using legitimate interests as a legal basis for processing personal data

You will need to use this guidance:

- When customising a privacy notice to ensure it complies with current data protection legislation.
- When conducting a 'data protection impact assessment' (DPIA).
- When otherwise collecting or receiving personal data for a new initiative.

Definitions

- Personal data
- Special Categories
- Data subject
- Processing

7.1. Processing in the legitimate interest

If personal data is to be used for purposes that do not relate to the College's core functions or public tasks, processing may also be possible if it is necessary for the legitimate interest of the College or a third party and does not negatively affect the rights and freedoms of the people whose data you are processing. Thus, this legal basis requires a balancing of the legitimate interests of the College and/or the third party against the interests and fundamental rights of the data subject. When performing this balancing test, you will always need to consider the data subject's reasonable expectation of what is likely to happen to their personal data. Processing must also meet the strict requirements of being 'necessary.'

Moreover, if you rely on legitimate interest, you will need to be aware of and make provisions for data subjects' right to object to the processing. This means that if somebody can prove that their own rights and freedoms outweigh the College's, then their objection to processing must be considered and they must be opted out of the processing. Data subjects must be informed of this in every processing communication they receive.

7.2. What is 'interest'?

An 'interest' is the broad stake the College may have in the processing, or the benefit that the College derives, or which society might derive, from the processing. It must be real and not too vague.

Some interests are likely to be legitimate because they are 'strictly necessary' for College administration or related legal compliance issues, particularly where there is no legal obligation to comply with, but the processing is essential to ensure the College meets external or internal governance obligations.

Example:

Fraud prevention *- where the processing is strictly necessary for the purpose of preventing fraud. This could include verifying that the registered address of the cardholder for a particular credit or debit card is the same as the cardholder's normal place of residence or work.*

Other interests are legitimate because they are a routine part of the activities of the College but other lawful reasons for processing are not practical or are not available.

Example:

Alumni newsletter *- a regular newsletter to alumni could be sent with consent as the legal basis. However, since consent requires a positive indication, an opt-in, it is not practical to ask for consent. Experience has shown that the return is minimal. It is also unlikely that alumni's rights and freedoms would outweigh the College's interest in sending regular updates.*

Regardless of the importance of the processing activity to the College, an assessment must be made to ensure the processing meets the threshold required to rely on legitimate interests as a legal basis.

7.3. When is processing in the 'legitimate interest'?

Below are some generic examples of processing that will usually be in the legitimate interest:

Reasonable expectations - the fact that individuals have a reasonable expectation that the College will process their personal data for this purpose will help the make the case for legitimate interests to apply when conducting the balancing test.

Relevant & appropriate relationship – where there is a relevant and appropriate relationship between the individual and the College, such as between the College and its alumni.

Network & information security – where the processing of personal data is strictly necessary and proportionate for the purposes of ensuring network and information security.

Suppression lists – once somebody has opted out of receiving communications, the College will keep a suppression list to ensure that the individual will not be contacted again. Keeping this suppression list is in the legitimate interest of the College.

7.4. How to carry out the legitimate interest assessment

To rely on its legitimate interest, the College must perform a three-stage assessment:

1. identifying a legitimate interest,
2. establishing that the processing is 'necessary' and
3. conducting a balancing test.

The legitimate interest can be one of the College or of a third party to whom the data may be disclosed, if the three-stage test is passed.

Once the assessment has been completed, and approved by the DPO, and the decision has been reached that 'necessary for the legitimate interest' is indeed the appropriate legal basis for processing, a concise summary of the reasoning behind the decision must be included in the privacy notice.

1) Identifying a legitimate interest:

The first stage is to identify a legitimate interest – what is the purpose for processing the personal data and why is it important to the College? A legitimate interest may be elective or business critical and can be those of the College or a third party to whom the personal data may be disclosed. It is possible that several parties may have a legitimate interest in processing the personal data. While you may only need to identify one legitimate interest, all relevant interests should be considered.

2) Carrying out a necessity test

You will need to consider whether the processing of personal data is 'necessary' for achieving the objective(s). The adjective 'necessary' is not synonymous with 'indispensable' but neither is it as wide as 'useful' or 'desirable.' It may be easiest to simply ask, 'Is there another way of achieving the identified interest?' If there is no other way, then clearly the processing is necessary. It is, however, not enough to argue that processing is necessary simply because you have chosen to operate your business in a particular way. If there is another way but it would require disproportionate effort, then you may determine that the processing is still necessary. If there are multiple ways of achieving the objective, then a DPIA should be used to identify the least intrusive processing activity. Finally, if the processing is not necessary, then 'legitimate interest' cannot be relied on as a legal basis for that processing activity.

3) Carrying out a balancing test

The College can only rely on a genuine legitimate interest where the rights and freedoms of the individual whose personal data will be processed have been evaluated, and these interests do not override the College's legitimate interest. Thus, you must carry out a balancing test.

This balancing test must always be conducted fairly, which means that you must always give due regard and weighting to the rights and freedoms of individuals.

There are several factors to consider when deciding whether an individual's rights would override the College's legitimate interest. These include:

- the nature of the interests;
- the impact of processing;
- any safeguards which are or could be put in place.

The **nature** of the interests includes:

- the reasonable expectations of the individual: would or should they expect the processing to take place? If they would, then the impact of the processing is likely to have already been considered by them and accepted. If they have no expectation, then the impact is greater and is given more weight in the balancing test;
- the type of data: special categories of personal data is subject to stricter rules on its use. This must be a consideration in a balancing test, and
- the nature of the interests of the College (e.g., is it a fundamental right, public or other type of interest):
    - Does it add value or convenience?
    - Is it also in the interests of the individual?
    - If there may be harm because of the processing, is it unwarranted?

The **impact** of processing includes:

- any positive or negative impacts on the individual, any bias or prejudice to the College, third party or to society of not conducting the processing.
- the College needs to carefully consider the likelihood of impact on the individual and the severity of that impact. Is it justified? A much more compelling justification will be required if there is the likelihood of unwarranted harm occurring.
- the status of the individual – a customer, a child, an employee, or other.
- the ways in which data are processed, e.g., does the processing involve profiling or data mining? Publication or disclosure to many people? Is the processing on a large scale?

Any **safeguards** which are or could be put in place include:

- a range of compensating controls or measures which may be put in place to protect the individual, or to reduce any risks or potentially negative impacts of processing, identified through a DPIA, for example:
    - data minimisation
    - de-identification
    - additional layers of encryption
    - data retention limits
    - restricted access
    - opt-out options
    - anonymization
    - encryption, hashing, salting

When the College is processing personal data relating to children, or special categories of personal data, particular care should be taken with the balancing test, as it may need to give additional weight to the rights of the individual.

7.5. The 'necessary' test

This guidance is for any member of College staff tasked with determining the legal basis for processing personal data

7.5.1. The legal basis

If you decide that you are processing personal data under any of the following legal basis, you will need to ensure that processing is indeed 'necessary' for its purpose:

- processing is **necessary** for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract;
- processing is **necessary** for compliance with a legal obligation to which the controller is subject;
- processing is **necessary** to protect the vital interests of the data subject or of another natural person;
- processing is **necessary** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is **necessary** for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, where the data subject is a child.

7.5.2. What does 'necessary' mean in a data protection context?

Before processing personal data, we will often need to show that doing so is 'necessary' to fulfil a specific requirement. For example, we may need to show that processing personal data is necessary to protect someone's vital interests.

'Necessary' means the data processing is a reasonable and proportionate necessity. It is more than desirable or convenient, but less than indispensable. The data processing is not necessary if the purpose can be achieved by a less privacy invasive method, by some other reasonable means or if the processing is necessary only because the College has decided to operate its business in a particular way.

Example

The College processes personal data about staff to employ them. The College does so on the basis the data processing is necessary to fulfil staff contracts of employment and to comply with the College's legal obligations as an employer.

However, if the College were considering outsourcing its HR functions to an overseas company and transferring staff data to that company, it is very unlikely the overseas transfer would meet the necessity test.

Specialised guidance

This data protection guidance has been produced for staff by the College Data Protection Officer (DPO).

1. International Data Transfer

Guidance regarding transferring personal data from the College to a country outside the UK

This guidance is intended for College staff who send personal data from within the College to an institution, a person, or an organisation outside the UK.

Introduction

The UK General Data Protection Regulation (UK GDPR) sets out that personal data may only be transferred outside of the UK when certain safeguards are in place. These safeguards are divided into two categories: 'regular' safeguards available to all data controllers and the so-called derogations, the exceptions that are only available to public authorities if the transfer falls outside their public tasks. Therefore, activities which the College has no delegated powers to undertake can continue to make use of these derogations to simplify overseas data transfers. However, teaching and research are public tasks, which the College has delegated authority to undertake.

Please note that transfer of personal data into the UK is unproblematic, as Data Protection Laws will apply as though the data were generated inside the UK.

Please note that accessing College systems by a College staff member from abroad does not constitute international data transfer although accessing College systems via an unsecured open 'Wi-Fi' network may compromise College systems.

Context

Under the UK GDPR and DPA 2018, these safeguards are not required where the European Commission ("the EC") has decided that a country, territory, or a sector(s) within a country has an adequate level of protection ("an adequacy decision") over personal data. Where an adequacy decision is available, transfers of personal data can take place as if the recipient were located within the EEA ("the EEA"), i.e., no further actions are required other than general compliance with the legislation. The UK recognise and has adopted these adequacy decisions; in addition, the UK will recognise all EEA countries as adequate.

To date, the EC has recognised Andorra, Argentina, Canada (only commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and Japan as providing adequate protection. Many of the College's oversees partnerships allow for the free transfer of personal data, as these involve institutions/bodies within the EEA. However, the College also shares personal data with institutions in countries with no EC adequacy decisions in place.

Please note that the EU has recognised the UK as adequate post Brexit.

Several scenarios involve the transfer of personal data outside the EEA and the adequate countries:

- Regular student exchange
- Teaching and/or activities delivered by an institution overseas
- International research collaborations
- International conferences and events
- Work placements
- External examiners
- Student or staff references
- Providing membership data to professional organisations or similar organisations
- Overseas development and alumni work

- Providing data to an embassy for a very important person (VIP) visit

The legislation lists 8 safeguards, at least one of which must be put in place to allow for the lawful transfer of personal data to non-adequate countries.

Adequate safeguards may be provided for by:

1. a legally binding agreement between public authorities or bodies;
2. binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
3. standard contractual clauses adopted by the EC;
4. standard contractual clauses adopted by the Information Commissioner's Office (ICO);
5. compliance with an approved code of conduct approved by the ICO;
6. certification under an approved certification mechanism as provided for in the GDPR;
7. contractual clauses agreed authorised by the ICO;
8. provisions inserted into administrative arrangements between public authorities or bodies authorised by the ICO.

Please note: The decision by the European Court of Justice from July 2020 invalidated the Privacy Shield for data transfer to the US and added requirements for use of the standard contractual clauses to be inserted into contracts unless another safeguard applies, or a derogation can be used. A risk assessment must now be completed and approved by the respective Director or Support Area Head of Department or their representatives whenever these clauses are to be used.

Besides the 8 safeguards, there are 7 derogations, which are alternatives to the application of a safeguard. It is important to note that the derogations are exceptions and must be used accordingly, only where necessary for exceptional situations and not for regular data transfer. Where available, a derogation can only be relied upon when there is no adequacy decision and application of a safeguard is not possible, or desirable, e.g., establishing a contract between the College and another party for a one-time transfer would not be an efficient use of resource; with no guarantee that the partner would accept the terms a proposed agreement.

The derogations are:

1. the individual's informed written consent;
2. necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
3. necessary for the performance of a contract made in the interests of the individual between the controller and another person;
4. necessary for important reasons of public interest;
5. necessary for the establishment, exercise, or defence of legal claims;
6. necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
7. made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

Note that the first three derogations, explicit consent and the two contractual derogations, only apply to the College's so-called private tasks, i.e., any task outside teaching and research.

2. Safeguards for international transfer – individual situations

2.1. Regular student exchange (incoming and outward-bound students):

- If the other educational organisation is a public body: a legally binding agreement between public authorities

- If the other College is private: necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.

2.2. Teaching and/or activities delivered by an institution overseas:

Teaching and/or research activities delivered by an institution overseas that rely on a personal data transfer from the College fall outside the scope of our GDPR compliance, as the College will not be undertaking any activities under its own powers – it will be the other institution that is doing so.

2.3. International research collaborations:

If the other College is a public body: a legally binding agreement between public authorities.

If the other College is private: standard contractual clauses.

2.4. International conferences and events:

Informed written consent.

2.5. Work placements:

Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.

2.6. External examiners:

Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.

2.7. Student or staff references:

Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.

2.8. Providing membership data to professional organisations:

Informed written consent.

2.9. Overseas development and alumni work:

Informed written consent.

2.10. Providing data to an embassy for a VIP visit:

Necessary for important reasons of public interest.

3. Research and data protection

Guidance on research and data protection legislation. The UK General Data Protection Regulation (UK GDPR) along with the Data Protection Act 2018 (DPA) sets out how personal data and privacy should be managed. The legislation applies to any research project which processes personal information. This also applies to research outside the UK that the College is involved in.

Undertaking research in an ethical, fair, and lawful manner, complies with the requirements for data protection legislation and must start prior to project approval by incorporating data protection and privacy into the research planning process. This guidance is intended to assist researchers with this.

3.1. Storing research data

Research data planning is an important part of ensuring your research is conducted in a way that is compliant with data protection, freedom of information and record management requirements.

The IT department can offer advice and tools to help you manage research data.

4. Anonymisation of personal data

Guidance on the anonymisation of personal data and when and how to do it.

What is anonymisation?

Anonymisation is the complete and irreversible removal of any information that could lead to an individual being identified, either from the removed information itself or this information combined with other data held by the College.

When should I anonymise information?

Data protection law regulates the handling of "personal data" which is information about living, identifiable individuals. It is good data protection practice to limit the number of people that have access to personal data. In some cases, this can be done by anonymising the information. When personal data is to be shown to a wider audience it will be, in most circumstances, appropriate to anonymise it.

Example scenario 1

Student Support have set retention times for all student records they keep. Once that retention time is over, they can delete the names, addresses and student numbers from the records. If there is no way for individual students to be identified through other means, such as, for example, the only female student in a class of 5, then they can retain the anonymised data sets for statistical analyses.

How can I be sure that I have completely anonymised information?

Anonymised data means that all identifiers have been irreversibly removed and data subjects are no longer identifiable in any way.

Information is fully anonymised if there are at least 3-5 individuals to whom the information could refer. For example, if your data relates to an individual of a specific gender and ethnicity living at a certain postcode you can increase the number of people to whom it could refer by only using the first 3 digits of the postcode.

Is anonymised information still 'personal data'?

No, if the information has been fully anonymised it is not personal data and therefore not covered by the Data Protection Act.

What do I do if I cannot fully anonymise information?

Full anonymisation is often difficult to attain. In most cases the information can only be partially anonymised and therefore will still be subject to data protection legislation. If you cannot fully anonymise information, it is still good practice to partially anonymise it as these limits the ability to identify people.

Partial anonymisation and pseudonymisation

Full anonymisation is often difficult to attain and for research, often not desirable. In most cases the information can only be partially anonymised and therefore will still be subject to data protection legislation. If you cannot fully anonymise information, it is still good practice to partially anonymise it as these limits the ability to identify people, or to pseudonymise.

Pseudonymisation is a privacy-enhancing technique; it is a process rendering data neither completely anonymous nor directly identifying. With pseudonymisation you separate personal data from direct identifiers so that linkage to an identity is no longer possible without the additional information that is held separately. It is important to note that pseudonymised data is not exempt from data protection legislation.

If you pseudonymise a research dataset by keeping the data and the identifiers separate and send the pseudonymised data to another College without also sending the identifiers, then the other College will process anonymised data. You, however, will still process personal data as you can still at any time re-identify individuals.

Example scenario 2

If you remove people's names from a dataset about College students, but leave their student number, the information has not been anonymised, as it is still possible to identify the people concerned. However, it will be more difficult for the people working with the dataset to identify them.

Example scenario 3

You are working on a research project that involves data about people, not everyone involved in the project may need to know the identity of the research subjects. If you are giving a presentation about the research, it is extremely unlikely that the identity of the subjects, or information that could lead to them being identified, is necessary for the presentation.

More guidance

The Information Commissioner's Office (ICO) has produced a Code of Practice on Anonymisation which provides detailed guidance. Please download this through the following link:

ICO Code of Practice on Anonymisation

5. Third party software application and services

Guidance for College staff on data protection and information compliance issues for using a specific piece of cloud software or services.

Before you start using any new third party-based software or services for College business, you must carry out due diligence to ensure that College information will be secure and appropriately managed.

This guidance is relevant to software or services where the College intends to transfer data to the relevant service provider, so it is hosted in the cloud, as well as the use of cloud based or other software where the College asks users to provide data directly to a software or service provider.

This checklist covers some of the main points you need to consider from a data protection and records management perspective.

Before you start

Check with the Information Technology and Reporting & Information Management (within IE (Institutional Effectiveness)) teams if any existing centrally supported College software meets your requirements. This will usually be the simplest option.

Checklist

a. Personal data must be stored inside the UK or in a country approved by the European Commission as offering adequate protection for personal data. (This includes personal data held on back-ups and anyone accessing personal data remotely). If the company is not able to guarantee this, you should not use the cloud service. Refer to International Transfers for list of approved countries.

If the company is based anywhere else, you will have to complete an International Data Transfer Assessment. Refer to International Transfers for list of approved countries.

b. Does the company offer an appropriate level of security for the sort of data that will be processed by the cloud service? Consider the level of security needed for personal data and any other sensitive College information, as well as the risks to the College or data subjects if the data was lost or damaged. Contact the Information Technology team for advice.

c. Will you be able to manage information retention?

- Is it possible to delete or take down information once your need for it has ended?
- Will the service provider remove information once their need for it has ended?
- If you need to keep the information for many years (e.g. because of research funding council policies on data retention), does the external service provider have arrangements in place to ensure the long-term survival and security of the data despite risks such as technological obsolescence and software and data standard changes, or is it possible for you to make arrangements to preserve the data yourself locally?

d. Are the terms and conditions and privacy policy of the company acceptable? You should always read the terms and conditions and privacy policy in full before signing up to any cloud service. Be aware that many cloud service provider supplier will be reluctant to negotiate terms.

e. The company must agree to sign an appropriate data processing or data sharing agreement. The standard terms and conditions and privacy policy of most cloud service providers are not normally sufficient, although some companies may not be willing to negotiate. The College DPO can provide advice and template agreements.

f. Carry out a data protection impact assessment (DPIA) for your project.

Data protection impact assessment guidance

Approvals

Once you have identified your service or Cloud based system, you will be required to present your Business Case to the Business Systems Change Committee (BSCC). Ensure you obtain the appropriate approvals. This must include agreement from the owner of data, for example if your project involves sharing personal data about students from the CreaTech Faculty, it should be approved by the relevant Delivery Director of CreaTech.

You also need to make sure you comply with any relevant College procurement regulations.

Procurement department website

6. Marketing, Publishing, and Communication

Guidance on data protection issues relating to mailing lists, photography, direct marketing and publishing personal data on the internet.

6.1. Mailing lists

Guidance for staff working with external and internal mailing lists.

This guidance is intended for all College staff who maintain and use mailing lists.

It is important to distinguish between mailing lists used to send communications for:

- **Marketing**: sending information seeking to persuade someone to buy something or to promote your aims, even for a not-for-profit body.
- **Services**: messages which are essential for the service you are providing (service news, updates, newsletters, announcements, …).

It is also important to distinguish between mailing lists used to communicate:

- **Externally**: sending communications to individuals from outside the College.
- **Internally**: sending communications to staff and students.

When you maintain and use a mailing list, you must always have a legal basis. There are different requirements for mailing by paper and electronic mailing and for marketing messages and service communications.

6.2. Privacy of emails

Ensure that you do not reveal the names and email addresses used for the email distribution to the recipients – **use 'bcc,' not 'cc.'**

Also, for email lists, it is best practice that the email originates from a genuine verifiable @activatelearning.ac.uk address rather than one created by an external third party.

6.3. External mailing lists

External mailing lists in paper format. If your mailing list is used to send communications in paper format to individuals external to the College, you do not need to obtain consent. Instead, the legal basis is 'legitimate interest.'

You must, however, provide recipients with the opportunity to easily and effortlessly, opt out of receiving the communication in every letter. This can be a phone number or an email address.

6.4. External mailing lists in electronic format

If you send emails to individuals external to the College, you must distinguish between sending communications to private individuals and to business contacts.

Business contacts ("B2B")

Business contacts are individuals who can be considered as representatives of their company, organisation, or institution, such as students or academics from another College, or professionals from all sectors. For B2B communications you can use "legitimate interest" as an appropriate legal basis and will not have to ask for consent. However, you must provide the option to opt out in every communication, for example through an 'unsubscribe' link in the footer of the email.

Private individuals

If you send emails to private individuals, then you must have obtained consent. This consent can be through people actively signing up to receive a newsletter through your website, by ticking a box when registering online for an event or signing up to a mailing list during an event.

If an existing mailing list exclusively or mostly contains private individuals who have not actively subscribed but have been added to the list for another reason, then you must request consent and remove those who do not reply from the list.

Renewing consent

Consent does not last forever and after an appropriate period must be refreshed. From the nature and content of the communications you must assess and determine an appropriate length of time after which you will re-consent subscribers. This could be anything between 2 and 5 years.

Always provide the option to opt out in every communication, for example through an 'unsubscribe' link in the footer of the email.

"Soft opt-in"

If the individual has bought something from you such as a product or a service, or attended a paid event, or is or has been in negotiation with you about buying a service, product or attending a paid event, then you do not need their consent to send emails to them about similar products, services or events as long as you give them the option of opting out of receiving marketing emails when you obtained their email address, and you provide an opt out or 'unsubscribe' option every time you send an email.

Suppression lists

If someone asks you not to send them marketing emails, then you must stop but you also must retain their email address for the purpose of ensuring they do not receive marketing emails from you again. This is known as a "suppression list" and the legal basis for maintaining the list is 'legitimate interest.'

6.5. Mixed lists

If your mailing list contains both B2B contacts and private individuals, a pragmatic, risk-assessed approach is recommended. If you have obtained valid consent originally, then you will not have to ask subscribers to re-consent. If you have not obtained consent from the private individuals, conduct a risk assessment to determine whether continuing to send emails is likely to cause offence or distress or whether receiving the emails are in the individuals' interest and/or to their benefit.

Always provide the option to opt out in every communication, for example through an 'unsubscribe' link in the footer of the email.

6.6. Internal mailing lists

Most internal mailing lists will be in electronic format. You need to distinguish between lists used for essential business and mailing lists used for other purposes

Essential business mailing lists

Essential business mailing lists will include information such as changes to lecture theatres for students, information about student assignments, information about facilities such as a lack of heating or power failure in certain buildings, or College closure due to snow. These mailing lists can be College-wide, Faculty or Team-specific, or programme-specific. Due to the nature of the information contained within these emails, subscription is mandatory and an option to unsubscribe

cannot be given. The legal basis for these emails is the 'contract' the College has with its students and staff provide a service.

6.7. Other mailing lists

Other mailing lists may include non-essential information about, for example, events on a Campus, within a faculty, or career opportunities for students.

Because staff members and students are business contacts, you do not need consent to send these emails, the legal basis for these emails is 'legitimate interest.'

For non-essential emails, always provide the option to opt out in every communication, for example through an 'unsubscribe' link in the footer of the email. You should maintain a suppression list to ensure you do not send any further emails to staff and students who have opted out.

6.8. Mixed content

If internal mailing lists include both essential and non-essential information, then they are treated as though they only contained essential information as the importance of providing this type of information overrides the requirement to provide the option to opt out of non-essential communications.

For these, no 'unsubscribe' link is required.

7. Photography

How to comply with data protection requirements when taking photographs and publishing photographs on the internet and internally.

Whenever individuals can be identified by their image, data protection legislation applies. In these situations, the rights of the individuals in the collection and use of their photographs must be respected – they must be informed when an identifiable image of them will be or has been captured, and a legal basis must be found before the image is used in any way.

7.1. Photographs of individuals and posed groups

When taking photographs of a specific person that you might want to publish on the internet, you can use 'legitimate interest,' 'consent' and 'contractual obligation' as your legal basis.

The ICO recommends using 'legitimate interest' as this is the easiest legal basis if that is valid and used correctly.

If you use 'consent,' then ensure that consent is validly collected and stored. Put this consent in writing using the attached consent form. This provides added protection for limited administrative effort. If children under the age of 13 years are clearly recognisable in an image, consent from a parent or guardian should be obtained. The consent form needs to be kept for the life that you hold the photo as evidence. If a data subject withdraws their consent, then the consent is still deemed to have been valid up to the point of withdrawal. The example the ICO gives is that if you had used a photo (on the lawful basis of consent) in your new prospectus and a data subject withdraws their consent, you do not need to take any action on all the prospectuses that you have sent out or distributed but you would not be able to use any more of the thousands of copies of prospectuses you still have. If you had sent the proof to the printers and they had already started production, you would need to cancel production and pay all the associated fees. If the photograph is on display in a public area such as a photo board, it must be removed as soon as possible.

Taking and publishing photographs can also be part of a contract, for example the keynote speaker at a conference.

In all three situations you must tell the data subjects what you intend to do with the photographs, including that they will be published on the internet.

7.2. Photographs of crowds or groups

If crowd shots are taken during an event and an individual is not identifiable, then there is no need to find a legal basis to take, display or publish the photo. This applies to any individuals, students, and staff whose images are incidental detail, such as in crowd scenes for graduation.

If the photos are taken at a conference where it is likely that individuals may be identified even in crowd scenes, then your legal basis is 'legitimate interest.'

In both these scenarios, you must include notices at the event informing attendees of the following points:

- Alert people in the foreground of these shots who are within earshot of the photographer verbally and given the opportunity to move away if they wish.
- Give a warning in writing that photography will be taking place at the event.
- If you use a registration form, then this warning must be included in the form, you can also use notices displayed at events and
- Include a sentence about photography in printed programmes or publicity material.
- Provide a clear opt-out (e.g., speak to the photographer, wear a sticker /wristband, remove yourself from the photo areas, say no thank you if the photographer asks, or event do not attend the event). Obviously, there can be practical challenges to this and there is a point where a photo is just a scene shot and no-one is particularly identifiable. Evidence would need to be kept of the information that you provided to the data subjects (e.g., keep the email / the posters / the event form etc.).

If you take pictures of random groups of people, such as in general campus scenes, and there is a possibility that individuals might be identified when the images are posted on the internet, then your legal basis will be 'legitimate interest.' In this situation, you will not have to provide a privacy notice.

Note: If you upload photographs of identifiable persons onto the internet, you will highly likely have an international data transfer. Please consult the guidance on International Data Transfer.

International data transfer guidance

7.3. Photographs of children

If taking photographs of children, you can use 'legitimate interest,' or you must obtain consent from a parent or guardian. This may be written or verbal depending on the circumstances, see the guidance above.

7.4. Photographs for ID purposes

Photographs are taken/provided by staff and students for identification purposes, as part of the College's contract with them to ensure their safety and security and to prevent fraudulent activity (e.g., exam or other identification). However, use of photographs beyond these purposes requires consent.

7.5. Photographs on intranet, internet or building notice boards

Profile photographs of staff or students on the College SharePoint or other sites that are restricted to current College staff and students require consent. The same applies to profile pictures on building notice boards.

Contact Marketing for the consent form for the use of profile pictures on intranet and building notice boards.

Publication of photographs of staff or students on internet sites or noticeboards that are accessible by public requires consent as a safeguard of the individual as this is considered international transfer (see International Data Transfer Guidance above). Use the template consent form below.

Individuals retain the copyright to their photographs and can withdraw consent at any time for their use. This is an example of a consent form staff can use. You must adapt it as appropriate to the circumstances.

Contact Marketing for the Photography and video consent form template.

Marketing and Communications have a privacy notice for photography and video which can be used alongside the consent form. The privacy notice is available on the Privacy Notices webpage.

8. Direct marketing

Guidance regarding marketing and data protection.

This guidance is intended for all College staff who maintain or use databases of contacts for 'marketing' purposes, including publicising events and programmes, fundraising, alumni activities and offering goods for sale

8.1. Background

Direct marketing only applies to targeting named individuals – for example, letters addressed to 'the occupier' would not qualify. It applies to communicating the advertising or marketing of commercial products or services, it also applies to fundraising, and includes all messages promoting an organisation or its values or beliefs. This could include information promoting College events such as conferences, or opportunities for students. Direct marketing covers all forms of communication, such as marketing by letter, telephone, email, and other forms of electronic messages. It is important to also note that any activity where the aim is to send marketing, i.e., activities that lead up to, enable or support the sending of direct marketing, is already considered part of your direct marketing. Examples are lead generation, data enrichment, matching or screening.

8.2. Requirements for all forms of marketing

Any personal details collected and held for direct marketing purposes must comply with the data protection principles. This means that you must always:

- Inform data subjects in your privacy notice that you will use their personal data for marketing purposes, also of the way they will be contacted (letter, telephone…)
- Have a legal basis for processing the data
- Not keep the information for longer than necessary
- Hold the information securely.

If you have acquired contact details from a third party for marketing, you must check the following:

- What information about the use of the data was provided at the time the data was collected?
- Did the individuals indicate any preferences about their means of contact?
- How have unsubscribe requests been handled?
- How has the list been kept up to date?

If you have collected personal data from public sources such as LinkedIn or other websites, you must provide privacy information when you first communicate with the individual, but no later than one month from the date of collection. You cannot assume that simply because an individual has put their personal data into the public domain, they agree to being contacted for direct marketing.

If you want to rely on the so-called 'disproportionate effort' exemption, you must assess and document whether there is a proportionate balance between the effort involved in for you to provide privacy information and the effect the processing has on the individual. The more significant the effect is likely to be, the less likely it is that you can rely on this exemption.

The law distinguishes between direct marketing using electronic means and non-electronic means and has different requirements for both. Currently, 'electronic means' covers the use of email and text messaging.

8.3. Marketing by non-electronic means:

Marketing by letter

If you intend to send marketing information to named individuals by letter, you can rely on 'legitimate interest' as your legal basis. All letters must include clear information on the identity and contact details of the data controller. Data subjects must also be made aware in every letter that they can

object to the processing and given information on how to do this, i.e., that they can 'opt out' of receiving further letters by phoning a free number or sending an email.

Marketing by telephone

If you intend to contact individuals for marketing purposes by telephone, you can also rely on 'legitimate interest' as your legal basis. In all calls, staff must identify themselves and, if requested, provide an address or telephone number on which they can be reached. Data subjects must also be made aware during every telephone call that they can object to the processing by phoning a free number or sending an email, i.e., that they can 'opt out' of receiving further calls.

Before making a telephone call, you will always need to make sure that the individuals are not registered with the Telephone Preference Service. If they are, you cannot rely on 'legitimate interest' but will need consent to contact them.

You can check here:

Telephone Preference Service

Marketing by electronic means

In addition to the UK GDPR, the Privacy and Electronic Communications Regulations 2003 (PECR) regulate in detail the use of electronic communications for marketing such as by email or text messages (SMS).

Electronic marketing to private individuals can only be done with consent as the legal basis. Consent must be 'opt-in,' must fulfil the UK GDPR requirements for consent, and any direct marketing messages should only be sent to those people who have in fact opted in to receiving such communications. All subsequent marketing communications must contain an option to opt-out of receiving further communications with details of how to do so, such as an 'unsubscribe' link at the bottom of an email. If you receive an opt-out request in relation to marketing, you must comply as soon as possible, there are no exceptions to this.

When requesting consent, it is good practice to request consent separately for different forms of communication i.e., whether individuals agree to be contacted via post, telephone, or email. This is because the different forms of communication are covered by different legislation.

Soft opt-in

One exception to the need to obtain prior consent is the so-called 'soft opt-in,' which is based on 'legitimate interest.' Soft opt-in can be used in situations where you have a pre-existing commercial relationship with the individual: the individual has bought goods from you before, has used services you offer, has attended, and paid for an event you have organised, or has been in negotiations with you about any of these with you. In these cases, you can market similar goods, services, or events to the individual without consent, however, you must have informed people when you collect their data that there will be marketing and that they can opt out.

Also, this will only ever apply to commercial activities, i.e., where payment has been involved, it will not apply to, for example, free lectures.

Business-to-business marketing

If the individual you wish to market to is a business contact, then you will not need to obtain prior consent, rather, for so-called 'business-to-business (B2B)' marketing, you can rely on legitimate interest as an appropriate legal basis. Business contacts are all individuals who can be considered as representatives of their company, organisation, or institution, such as academics from another College or professionals from all sectors. You must, however, provide the possibility to unsubscribe in every email.

Marketing via tracking software through social media

If you wish to use tracking software, please consult the College's Cookie Policy and Procedure, where you will find detailed guidance. Cookie Policy

9. Removing Staff Contact Details from Public-Facing Webpages

Procedure for having contact details removed from public-facing website.

9.1. Background

The College aims to be open and transparent in all its proceedings and procedures. Part of this transparency is having the names and contact details of employees accessible through the College SharePoint and through the telephone and email register Outlook, and through the staff profiles and lists in the individual business units.

Note: this procedure only applies to contact details on the public-facing internet, not to any internal sites.

9.2. Who do I need to contact?

If you have a personal reason why your contact details should not be shown on a public-facing website, the request needs to be co-ordinated either through your line manager or, if you do not feel comfortable discussing the request with your line manager, with the local HR BP contact to ensure that your privacy can be protected.

Your line manager or the HR contact will make the initial assessment as to whether the data can be removed from websites by balancing the reason behind your request with the interests of the College. Guidance on this can be sought from the DPO, however, your line manager or the HR BP (Business Partner) contact will of course protect your privacy and not disclose your name.

If the request is approved, your line manager or the HR BP contact then takes the removal request to the relevant web editor(s) or team(s) responsible for making website updates. Ensure that you discuss with your line manager or HR contact where your name and contact details may appear, e.g., names in published committee papers. The updates may then be done directly or through the relevant Service Desk system (e.g., IT or P&E (Property & Environment) system) but a log will be retained of the action taken regarding the removal of the data.

Note: If you had originally given consent to having your profile photograph published on a public-facing website, you can withdraw that consent at any time to your line manager or local HR contact and have the photograph removed. If the photograph is only published on an internal site, you will need to provide a reason to your line manager or HR contact why you want to have the photograph removed and an evaluation will then take place, weighing your reasoning against the need to have your photograph visible to colleagues.

9.3. Updating personal information on web pages

You can request that the College updates or removes information about you on its web pages. This could be because of a name change or because you have left the College for example.

Who do I need to contact?

To request an information change or removal you should contact the website owner to request this.

Most areas of the College manage their collection and retention of personal information independently so contact the faculty or Group Service unit which holds it.

Not sure of the right contact?

If are unable to find contact details please contact the IT Services Desk detailing the change needed and the exact website address of the page containing the information.

Personal Data Processed by Students

1. Students undertaking research or other work involving personal data.

This guidance is intended for students undertaking research or other work involving information about living, identifiable individuals as part of their programme of study at the College

2. Background

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 protect the rights of individuals when you process personal data about them, including obtaining, holding, and destroying it.

The definition of personal data is extraordinarily complex. For day-to-day purposes, it is best to assume that all information about a living, identifiable individual is personal data. This includes any expression of opinion by or about the individual.

Students use personal data for three main reasons:

1) To maintain a personal life, for example to communicate with family and friends.

2) To pursue a course of study with the College, for example to research and draft an essay, report, or thesis.

3) To carry out research as a member of the College established research group.

Students may use many different methods to process personal data, such as maintaining an email account, a computer database, or using social media accounts.

3. The data protection laws and you

The College is only responsible for personal data when it is the data controller for that data. A data controller is the person who determines the purposes for which, and the way any personal data is or is to be processed. Therefore, the College is only responsible for the personal data processed by its students when the students process data for the College's purposes.

The following scenarios are the most likely circumstances in which students will process personal data.

Scenario one

Students process personal data during their personal life, for example drafting e-mails (using their College-provided e-mail account) to their families about a friend's recent birthday.

The College is not the data controller for personal data processed by students during their personal life, as the College does not determine the purpose of the processing. The fact that students may choose to use their College-provided e-mail account to pursue their personal life does not make the College responsible for the processing of personal data for that purpose. The College did not determine the purpose so the College cannot be the data controller. Students are the data controller and may claim the so-called ‘purely personal or household activity’ exemption. Use of this exemption has the effect that data protection laws do not apply to the processing activity.

Scenario two

A student processes personal data to pursue a course of study with the College.

The College is not the data controller for personal data processed by students to pursue a course of study with the College. Students undertake a course of study with a college for their own personal purposes, most obviously to obtain a qualification. Students are not employees or agents of the College, and neither do they act on behalf of the College. Students decide what work they will do, the way in which they will do it and what they will include in their final write up. They must make these decisions themselves to prove that they are capable of degree-level work. They work on behalf of themselves and not the College. Thus, the College cannot be the data controller for the personal data processed by students during their studies.

Again, the ‘purely personal or household activity’ exemption applies. However, the student will still be bound by the College’s policy and procedures due to the Student Contract with the College.

This means that when students are processing personal data as part of their work to pursue a course of study, the College's Data Protection, and Information Security Policy (linked below) applies to them and they will be required to ensure that their work complies with the data protection principles. This contractual duty to comply with the College's Data Protection and Information Security Policy extends to all work related to the course of study, even if the Student Contract has expired, such as a promise to inform research participants of results after the dissertation has been submitted and approved.

If the students use the work generated during their course of study as the basis for a post as academic researchers, then the College is the data controller for this follow-on work.

Data Protection and Information Security Policy

If the students use personal data in their research, whether for an undergraduate or postgraduate award, then they must complete a data protection impact assessment.

Data Protection Impact Assessment

Scenario three

A student submits a piece of work (e.g., an essay /report /dissertation /thesis) in which there is personal data, to the College for assessment.

The College and the student are joint data controllers for the personal data contained within the submitted piece of work from the point at which it is submitted. Once the work has been submitted the College is jointly responsible for the personal data within the document, for example the member of staff who marks the work is processing the personal data contained within it (by reading it) for the purpose of determining what grade the College should award the student; this is the College's purpose. If the work is then transferred to the College library to be put on reference the College is responsible for any processing of the personal data associated with the document being placed on reference as providing a reference service is a College purpose.

Scenario four

A research student processes personal data whilst working on a project led by a College research group. This scenario is only relevant for postgraduate research.

The College is the data controller for personal data processed by a student working on a research project led by a College research group. The student processes personal data for the purposes laid down by the project, the remit of which has been decided by the College (or the College employed project leader), not the student. The purposes for processing are the College's and not the student's; therefore, the College is the data controller, and the student is an agent of the College. This is the case whether the student is funded by the research project or whether the student is self-funding.

Scenario five

A research student processes personal data to pursue a course of study with the College. The College is the (co-)sponsor of the study.

In this situation the College will always be a data controller.

4. Conclusion

The College is the data controller for personal data processed by students only in extremely limited circumstances as described in scenarios 3, 4 and 5; in all other circumstances students process data for their own purposes and not the College's and are covered by the 'purely personal or household activity' exemption.

Ten steps to responsible use of personal data

1) Before you start, carefully consider what personal data you need to collect for your project and obtain the consent of your supervisor or other relevant member of College staff.

2) Obtain ethical consent from the data subject. For research this will usually be in writing. Discuss with your supervisor any concerns about obtaining consent prior to collecting personal data.

3) Give a clear explanation of what you are going to do with the data to the people participating in your research.

4) Do not collect or keep data that is not necessary for your research. Anonymise data where possible by removing names and other identifying information.

5) Ensure that all personal data, especially opinions, is recorded accurately.

6) Respect reasonable requests to update or delete data you have collected.

7) Store personal data securely. If you are using information that is already public knowledge such as the names of Olympic medal winners, you will not need to take any security measures. However, if you are recording less public information, you must ensure that the information is secure.

8) Do not disclose personal data to anyone except the individual concerned.

9) Securely destroy personal data when it is no longer necessary for your research. Consult the Assessment Regulations by contact your local Exams team, to confirm how long you will need to retain research data for until your marks have been confirmed.

10) Be aware of required safeguards for international transfers of personal data outside of the UK.

Data protection and social media

Social media is a valuable tool for staff and students, but use must comply with data protection laws.

1. Background

Social media provides important opportunities for staff and students to communicate and engage with a wide range of audiences and stakeholders. There are, however, a few data protection risks associated with the use of social media which could impact on the College's reputation.

These guidelines complement existing procedures and guidance from Human Resources, IT Services and Marketing.

Human Resources, in consultation with key stakeholders, has recognised the benefits of social media to the College and endorsed the use of social networking for positive engagement within our working environment and as a communication tool to share important news, updates and events. The main procedure can be found here:

Social Media Procedure

2. Social media and research

Re-tweeting posts

It is acceptable to re-tweet posts within your faculty or department Viva Engage (previously Yammer) or Twitter account, provided this would not be detrimental to the data subject and that the data subject is unlikely to object to the post being shared. In the case of re-tweeting, the information is already out in the public domain and an individual who has created an account on Twitter will have acknowledged at the time of creating their account what can and cannot be done, thus will have the expectation that their tweet will be re-tweeted. Of particular importance is also the Twitter Privacy Policy, which can be found here:

Twitter Privacy Policy

Security and Compliance in Viva Engage

3. Harvesting social media posts for research

Many research projects involve harvesting and analysing social media posts. While many of these will be in the public domain, the data protection requirements must still be adhered to. This means that the authors of the social media posts must be provided with a privacy notice within one month after harvesting them. That can be through, for example, a tweet to them. The same applies to all research using publicly available data – you still must adhere to the fairness principle and provide a privacy notice.

4. Tagging individuals when creating posts

You can tag individuals when creating social media posts as a person who has created a Twitter or public Facebook account will have acknowledged at the time of creating their account what can and cannot be done. However, you should only do this where the individual is unlikely to object to being tagged/associated with the post. You should not add or create any further identifiable or personal data about the individual that is not already publicly available without the individual's consent.

5. Social media and marketing

It is not acceptable to link to individuals' personal data (such as graduates' publicly available Linked In profiles) to market programmes. Although an individual's Linked In profile is publicly available, you cannot create any marketing materials that link to these profiles (which contain personal data) without the individual's consent.

You can publicise staff or student successes on your college or faculty social media site. Your legal basis will be legitimate interest and specific consent is not required, however if you are publishing a photograph of the individual, then consent for use of the photograph will be required (if not already obtained as part of staff/student photograph use).

Dealing with Subject Access Requests

1. Receiving a Request to Exercise a Data Subject's Right

Requests to exercise a right under GDPR may be made in any format, to any member of staff at the College at any time. Whilst we use the website to encourage data subjects to use our standard Rights Request Form, requests do not need to be made in writing. Staff should therefore be vigilant to requests to exercise these rights.

Upon receiving a request, you should:

2. Verify the Identity of the Requester

You should take reasonable measures to verify the identity of the person making the request. You may verify the identity of the requester in the following ways:

- requests made in person – ask if the requester can produce any photographic proof of ID. This may include a passport, driver's license, or College ID card. Check that the ID is in date and the photograph matches the requester;
- requests made over the phone – if you have access to the necessary information, check the requester's ID using security questions. Ask the requester to provide at least two pieces of information that only the data subject would be likely know, such as their date of birth and the name of their teacher; or
- requests made by email – check that the email address from which the email has been sent matches the contact details we hold for the data subject.

Requests made by third parties on behalf of a data subject – such requests must be accompanied by proof of the data subject's consent to the third party making the request, which must be verified by the DPO. If you are unsure or unable to confirm the identity of the requester, you should inform the DPO's office, which will conduct additional identity checks, as necessary.

3. Collect or Check Contact Details

Take a note of the requester's full name, telephone number and email address or, if you have access to the requester's contact details, ask them to verify the details are correct.

4. Take Details of the Request

Take as much information as possible about the nature of the request, including any specific information or data to which the request relates.

5. Refer the Request to the DPO

Assure the requester that you will pass on their request to the Data Protection Officer, who will contact them directly and will process the request. Complete the Rights Request Referral Form and forward it to the DPO immediately. The College is required to respond to all requests to exercise a data subject's right within 30 calendar days. It is therefore important that all requests are referred to the DPO without delay.

Staff should never attempt to fulfil a rights request directly. The only exceptions to this are simple rectification or withdrawal of consent requests, as outlined later in this procedure.

6. Verification and Confirmation of a Request

Upon receipt of a referral or direct request, the DPO's office will begin to process the request, as follows:

7. Verifying Identity

If the requester's identity has not yet been verified, the DPO's office will contact the individual directly to conduct this check. The type of identity check will depend upon the nature of the request, but may include:

- contacting the individual via contact details held by the organisation, other than the contact method used to make the request (e.g., via email if the request was made over the phone);
- asking two or more security questions;
- requesting an electronic copy of a piece of photographic ID; and
- requesting the supply of an original piece of photographic ID.

8. Verifying the Request

If necessary, the DPO's office will seek further information to verify the nature of the request, identify the specific data affected and ascertain the required method of provision of the data.

9. Confirming the Request

The DPO's office will then confirm the request to the individual in writing, outlining the process for fulfilling the request.

10. Identifying Relevant Data Sets

To process a Rights Request, the DPO's office will contact the relevant departments and teams who may hold information relevant to the request, including:

For students:	Institutional Effectiveness Group Administration Admissions / Student Support Learner Support Relevant Faculty/ies IT Marketing
For staff:	HR Relevant Department/Team IT
For business contacts:	Relevant Faculty / Department Marketing
For customers:	Marketing Admissions / Student Support

Under normal circumstances, the DPO will contact the relevant departments by sending a time limited Office365 link to a document containing details of the request. If the scope and nature of the request requires it, an all-staff email may be sent to ensure a thorough and complete response.

If applicable, the DPO's office will use the relevant Data Map(s) to ascertain whether the data has been shared with any third party and will contact that third party directly if necessary.

11. Staff Assistance with Rights Requests

Due to the response deadlines for Rights Requests, you are required to action any requests for assistance with a Rights Request without delay. Often, this will include conducting a thorough search of your data storage, including but not limited to:

- paper files;
- electronic files (documents, spreadsheets, etc.);
- databases;
- portable media and devices;
- notes and notebooks;
- emails;
- archives;
- text and phone messages; and
- noticeboards.

Please note that personal data includes all information that, either on its own or if combined with other data that College may reasonably hold, could uniquely identify the data subject. This will include any correspondence, documents or notes that refer to the individual in an identifiable way, as well as database entries.

Failure to conduct a thorough search, resulting in failure to supply, correct or erase the relevant data in a timely fashion could lead to the College breaching its obligations under data protection law, and therefore may be a disciplinary offence.

12. Procedures for Specific Types of Requests

12.1. Rectification Requests

If you receive a Rectification Request relating to data to which you have access and editing rights, and you have been able to verify the identity of the requester, you should amend the data immediately, confirm this to the requester, and contact the DPO, using the Referral Form, to inform them of the request and the action taken. In the case of simple rectification requests, verbal confirmation of rectification to the requester at point of request will be deemed sufficient. You should also inform the DPO of any third parties with whom the affected data has been shared. The DPO's office will take the necessary steps to check whether other copies of the data exist elsewhere and may also require rectification.

In the event of a Rectification Request which has not already been actioned, the DPO's office will contact the relevant department(s) directly to request that they amend the relevant data. Where that data has been shared with any third parties, the DPO's office will contact them directly. Upon receiving confirmation from the relevant departments and third parties, the DPO will write to the requester to confirm that their information has been updated.

12.2. Withdrawal of Consent

Where personal data is processed based on consent, this shall be recorded on the relevant data map(s) and complete records of consent given shall be maintained by the relevant department (usually Marketing or Institutional Effectiveness), in line with the relevant guidance. Customers will be provided with the facility to withdraw consent for direct marketing via the Preference Centre on the College website. Requests to withdraw consent submitted via the Preference Centre will be automatically actioned via the CRM system. Data subjects may also withdraw requests by simply making a verbal or written request. If you receive a request to withdraw consent you should, where possible, amend the preferences immediately to reflect the request and confirm this to the requester. If you do not have access to the database, please send the request through to the relevant department, who will action the request. In general, you do not need to inform the DPO when you receive withdrawals of consent; however, you should still contact the DPO if you are unsure about the request, or if it is combined with another rights request.

12.3. Subject Access Requests

To process a Subject Access Request, the DPO's office will contact the relevant departments (or in some cases, all College Staff) to request that they supply copies of all data they hold that is within scope of the request. The DPO's office will give a clear deadline for provision of the data, and you are required to compile the relevant data and provide it to the DPO's office in electronic format, as soon as possible and within the stated time limit.

When providing information for a Subject Access Request, you must inform the DPO's office of any data supplied that may be sensitive, either commercially, legally, or reputationally.

The DPO's office will compile all relevant data and redact the personal data of any other data subject from the data set. In some cases, where there is an exceptional volume of data involved, the relevant departments and/or faculties may be required to assist with the redaction of data.

The DPO will review the responses to all Subject Access Requests before they are issued and will check whether any data may be subject to exemptions which would prevent the issue of that data. Once the response has been approved by the DPO, it will be issued to the data subject in one of the following ways:

- electronically, via a time-limited link to a OneDrive folder, which will be sent to the data subject's email address and will expire within two weeks (this will be the default method); or
- physically, via recorded delivery post to the data subject's home address.

12.4. Erasure Requests

Upon receipt of an erasure request, the DPO's office will contact all relevant departments to identify what personal data is held and whether we are required to keep it by reason of an overriding legal basis for processing. Therefore, when identifying data, you should inform the DPO's office whether you consider it necessary to retain the data, and on what basis. Overriding legal bases will include contract, legal obligation, and public interest.

The DPO's office will inform the relevant departments of any data for which there is no overriding legal basis for retention, and staff will be required to permanently destroy, delete, or redact the data, and confirm to the DPO's office that this action has been taken.

Following confirmation of all necessary erasure, the DPO's office will write to the requester to confirm what data has been retained, and for what reason(s), and that all other data has been erased. The requester will be asked to give consent to a minimal amount of data being held on the Suppression List, so that, if a server backup must be restored, any personal data restored may be erased again. If the requester declines to give consent for their details being held on a Suppression List, their personal information shall be redacted from the records of the request, and the entry on the Requests Register shall be anonymised.

12.5. Portability Requests

The right to data portability applies only to electronic data which is provided directly by the data subject and is processed on the legal basis of contract and/or consent. Upon receipt of a data portability request, the DPO's office will refer to the relevant data maps to ascertain that the right to portability applies to the personal data included in the request.

If the right to portability does not apply, the DPO will decide whether to:

- refuse the request;
- comply with the request as a gesture of goodwill (in the case of requests that will require a minimal amount of work); or
- inform the requester of their right to submit a Subject Access Request in relation to the data.

If the right to data portability does apply, the DPO's office will contact the relevant departments to seek electronic copies of the data, which is to be provided in a machine-readable format as required by law; usually either an Excel spreadsheet or a CSV file. Once compiled, the data shall be transferred either to the requester or the specified third party, as per the request, usually by way of a time-limited file link on OneDrive, which will be sent to the data subject's email address.

12.6. Objection Requests

The right to object to processing applies only to direct marketing processing (including profiling) and processing undertaken because of legitimate interest or public task.

12.6.1. Direct Marketing

If a data subject objects to processing for the purposes of direct marketing, the DPO shall inform the Marketing department of the request immediately, and request confirmation that the personal data which is held for direct marketing purposes be erased from the CRM system. A minimal amount of personal data will be retained on a Suppression List, to ensure that future direct marketing activity is prevented. Any personal data held and processed for purposes other than direct marketing shall be retained and such processing shall continue.

12.6.2. Public Task or Legitimate Interest

Where a data subject objects to processing of their personal data which is undertaken based on legitimate interest or public task, they are required to provide an outline of the reasons for their objection. The DPO shall evaluate their request, balancing College's legitimate reasons for

processing the data with any risk or harm to the data subject. To conduct this evaluation, the DPO may seek the input of relevant departments such as Institutional Effectiveness and HR, as well as legal advice as necessary. The DPO may also take measures to restrict the relevant processing whilst the request is being considered. If the possible or actual detriment to the individual is considered to outweigh the legitimate reasons for processing, the DPO shall add the individual's details to the Suppression List and inform all relevant departments of the need to erase or cease processing the relevant data for the relevant purposes. Any personal data held and processed for purposes other than those identified shall be retained and such processing shall continue.

12.7. Restriction Requests

The right to restrict processing applies only in particular circumstances, such as when the data subject has submitted an objection or rectification request which is under consideration, or when the data is unnecessary or has been processed unlawfully but the subject does not want it to be erased. Requests for restriction are normally temporary.

If the restriction request is deemed by the DPO to be legitimate, they shall take necessary measures to prevent the processing of the information. This may include:

- requiring duplicate copies of the relevant personal data to be erased;
- collecting the relevant personal data and storing it in a secure location accessible only to the DPO's office;
- restricting access to the relevant personal data, if held on a database, to select members of staff who have clear instructions not to process the data;
- taking a backup of personal data from the relevant databases, which may be restored once the restriction is lifted; and
- adding the data subject to a Suppression List.

Once the period of the restriction has elapsed, the DPO's office will write to the requester to inform them that the processing of their personal information will resume, giving them no less than 5 working days' notice.

13. Administration and Response to a Request

The College is required by law to provide a response to all rights requests within one month of receipt or, if necessary, confirmation of identity. The deadline for response is therefore the corresponding calendar date of the next month (or the end of the month if there is no corresponding date). This may be extended by a further two months if the request is especially complex, or we have received several requests from the individual, in which case the requester will be informed of the extension immediately. Due to the response times for Rights Requests, the DPO will conduct all necessary checks, acknowledge the request, and contact all relevant departments for assistance as soon as possible. Upon receipt of a Rights Request, the DPO's office will log the request on the Rights Request Register, which will be kept updated as the request progresses. The DPO's office will conduct any necessary checks and acknowledge the request using the Rights Request Acknowledgement Template without delay. Where it has not been possible to complete the necessary checks, the DPO's office will inform the requester that the request will not be progressed until checks are completed.

The most accurate and appropriate way to identify data relevant is through staff reviewing the data they hold however, it may be necessary for IT Services to conduct a search of the Office365 system, to identify the location of relevant data. The DPO's office will request a preliminary search and review the results to identify relevant data; a more thorough search will then be conducted based on the preliminary results and the DPO's office will conduct a thorough assessment to identify data to be downloaded or deleted from the system. Once the DPO is satisfied that the request has been carried out, they will respond to the requester to confirm the outcome, using the Rights Request Confirmation Letter Template. This confirmation will include contact details for appeal and, if it is not possible to comply fully with the request, the reasons for this. The Rights Request Register will be updated and, if necessary, the Register and correspondence sent out during the rights request process will be anonymised or redacted.

Freedom of Information Procedure

The College collects and records information because of our daily activities and running of the business. As part of our commitment to openness and accountability, the College recognises its obligations under the Freedom of Information Act and the need to comply with the demands of the legislation. This section outlines the procedure for proactively publishing information under the Act and responding to Freedom of Information requests.

1. Scope & Responsibilities

The Data Protection Officer is responsible for ensuring that the College fulfils its obligations under the Freedom of Information Act, including the publication of information and responses to individual Freedom of Information requests.

However, this procedure applies to all staff of the College, and therefore staff should ensure that they are familiar with it and are therefore aware of the Group's commitment to the act and how it affects them. This may include notifying stakeholders or members of the public of their right to make a Freedom of Information request and how they should go about doing so. Staff should never respond to a Freedom of Information request directly but should take proactive steps to ensure that recorded information is readily available and accessible should a Freedom of Information request be made concerning that information.

2. Communicating Freedom of Information

College has two distinct obligations under the Freedom of Information Act. We must both publish certain information proactively, through use of the ICO's publication schedule, and we must respond to requests for information from the public. To perform these tasks, we must first communicate with the public to ensure that the information that we are able to provide is made known to anyone wishing to access it. To do this, we will publicise our commitment to proactive publication and the details of what is available, inform members of the public that they are able to make a Freedom of Information request and provide information about how to do so. It may also be necessary to communicate to staff at an early stage that each request will be considered individually and that we are unable to guarantee confidentiality of information released.

3. Publishing Information

The Freedom of Information Act requires that every public authority has a publication scheme approved by the ICO, which allows organisations to publish information proactively, as well as responding to requests. To this end, the ICO has produced a model publication scheme which the College will follow to publish information on the public website. The model publication scheme classes information into seven broad categories, however a definition document is available for further education colleges to give more detailed examples of the documents that should be published. There is no obligation on the College to publish drafts, notes, or obsolete versions of final documents.

The information provided on the Freedom of Information section of the public website will be reviewed on a regular basis by the DPO, so that both relevant newly created information is added to it and any superseded documents are replaced. It is the responsibility of the Directors of relevant areas of the business to provide these documents when requested and to inform the DPO when any of the documents change and require updating. Furthermore, the DPO will ensure that the responses provided to Freedom of Information requests are published on the public website also. Any disclosure under the Act is considered public disclosure, and therefore all personal information contained within the response must be removed or redacted prior to disclosure.

4. Responding to Requests

All formal requests under the Freedom of Information Act must be provided in writing, include a real name, and contact address and clearly attempt to describe the information being requested. This can be provided to any staff member and does not need to specifically mention the Act itself.

Any request made under the Act should be immediately referred to the DPO upon receipt. However, not every request for information will be a request under the Act; staff members receiving requests for information should carefully consider whether the request is:

- a request by a known third party who is entitled to receive the information, which can easily be provided directly, which should be handled by the relevant department;
- a request for personal information under the Data Protection Act (2018), which should be referred to the DPO as a Rights Request (see the Data Protection Policy and Rights Request Procedure for more information);
- a request made explicitly under the Freedom of Information, or which cannot be immediately fulfilled, which should be referred to the DPO as a Freedom of Information request; or
- a request for information which is already published under the Group's publication scheme, in which case the requester should be directed to the relevant section of the website.

Once a request has been received by the DPO, an acknowledgement letter will be sent without undue delay informing the requester that we are dealing with their request under the terms of the Freedom of Information Act. The only exceptions to this are: where the information can be provided immediately, either because the DPO has it to hand or because it exists in the publication scheme, in which case a response can be issued without need for an acknowledgement; or where further clarity is required, in which case it will be sought from the requester. If a formal Freedom of Information request is opened, we are obliged to respond to the request within 20 working days, which begins the first day after the request is received (or clarified, if applicable) by the Group. Information about the request will be entered into the Freedom of Information register by the DPO, who will then co-ordinate the communication of the request to relevant teams who are able to provide information to satisfy the request.

All information held by the College which falls under scope of the Act must be released, unless there is a good reason not to. Information will be provided as it was at the time of the request, regardless of whether the information is accurate or soon to be out of date.

College can refuse a Freedom of Information request in the following circumstances:

- where the cost of retrieving the information would be too great;
- where retrieval of the information would take too much time;
- where the requested information is not held by the College; and
- where an exemption listed under the Freedom of Information Act applies (in particular, where the request includes personal or commercially sensitive information).

The DPO will seek advice and conduct a public interest test to establish whether College has the right to refuse to provide requested information. This may involve a reasonable extension of time or no more than an extra 20 working days to consider. If a request is refused, the DPO will send a formal refusal letter to inform the request of this, informing them specifically under which section of the Act they are refusing to release the information.

Where the College is obliged to provide the requested information under the Act, the DPO will gather the relevant information and release it to the requester, either within or accompanied by a confirmation letter. The outcome of the request will then be detailed in the Freedom of Information register and the information provided will be uploaded to the public website. Future requests for the same information should subsequently be directed here.

Data Breach Procedure

If the security of personal data processed by the College is compromised, the organisation has a legal obligation to respond in such a way that minimises, where possible, the impact on the data subject. This procedure outlines the process for responding to data breaches and is intended to ensure that key elements are routinely addressed, including containment and recovery, ongoing risk assessment, data breach notification, evaluation, and response.

1. Scope

This procedure applies to all staff of the College, including its subsidiaries. The procedure applies to breaches affecting all personal data held or processed by or on behalf of the College, including, but not limited to data relating to students, staff, and external stakeholders.

2. Discovering a Data Breach

Data breaches come in a variety of forms and can be committed by anyone. Most data breaches are not malicious or intentional, but often occur because of genuine mistakes in the course of day-to-day work. Common examples of data breaches include, but are not limited to:

- emails sent to the wrong recipient containing personal data, either in the body of the email itself, or within an attachment to the email;
- emails sent to groups of people who have been Cc'd, rather than Bcc'd;
- paper copies of documents left unattended or accidentally disposed of;
- Stored documents damaged by accident;
- electronic devices containing personal data that are stolen, compromised, or taken outside of the EEA without prior approval; and/or
- information erroneously uploaded to the public domain, either due to the location of the upload or the privacy settings selected.

When a data breach or likely data breach is identified, it is essential that a prompt response is made and therefore the staff member who identifies it must inform the DPO immediately. This can be done via the linked Data Breach Notification form on the Staff Portal, or, if the breach is serious or urgent, by emailing the DPO at dpo@activatelearning.ac.uk. In some cases, the staff member who reported the breach and their manager, may be required to assist in gathering further information to assist the DPO's investigation and response.

3. Investigating A Data Breach

Upon notification of a potential / suspected breach and completion of the Data Breach Notification form, the details will be recorded on the Data Breach Register. Where necessary, the DPO will further investigate to ascertain the details of the situation. This includes:

- what data has been compromised;
- how many data subjects have been affected;
- where and how the breach originated; and
- the potential impact on affected data subjects.

To minimise any delay, the DPO may instigate remedial action whilst the investigation is ongoing. Staff members are required to provide prompt assistance in implementing any remedial action advised by the DPO, to minimise the impact and risk to the data subjects and College.

4. Risk Assessment

Once sufficient information has been gathered, the DPO will conduct a risk assessment (refer to Appendix 12) of the breach, considering the following:

- the number of subjects affected,
- the sensitivity of the data,

- the potential detriment to affected subjects and the,
- possibility or efficacy of remedial action.

The DPO may seek further advice from relevant staff members, legal advisors or the ICO to support this risk assessment.

Based on this risk assessment, the DPO will decide whether the breach is a:

- low risk breach, requiring no active response or remedial action;
- medium risk breach, requiring some remedial action, reporting and/or follow up;
- high risk breach, requiring a formal and coordinated organisational response.

In the case of low-risk breaches, where no further response is required, the case will be recorded and closed. Depending upon the nature of the breach, the DPO may recommend some follow up action, as described below.

5. Data Breach Response Team

In the case of a high-risk breach, a coordinated organisational response may be required, and this will be managed through a Data Breach Response Team, led by the DPO. If a Data Breach Response Team is required, this will consist of representatives of relevant departments (as applicable), which may include:

- Group Director for Institutional Effectiveness;
- Group Director for IT;
- Group Director for Digital Education;
- Head of HR Operations / Head of HRD;
- Group Director of Student Experience and Safeguarding;
- Group Director for Property and Environment;
- Head of Group Administration, Compliance and Health & Safety
- Group Executive Director for the affected faculty or division.

The DPO will contact each Director required in the instance, to inform them of the breach and call an Incident Response Meeting (which may be held via conference call as necessary). If the Director is prevented from attending the meeting and supporting the response, they are required to nominate one or more suitable representative(s) from their department. In some cases, the Director may wish to include members of their team with relevant skills and experience, such as the Designated Safeguarding Lead, the PR and Communications Manager, or the Property & Environment Manager.

The purpose of the Incident Response Meeting will be to:

- share details of the data breach and the outcome of the risk assessment;
- agree a Data Breach Action Plan to cover remedial action, notification, risk management and follow up, including assigning action points to relevant departments;
- agree arrangements for reviewing the situation and the progress of the Action Plan; and
- assess the level of public interest in the matter and the level of risk to reputation and where relevant initiate and agree a PR and Communications plan.

Where a Data Breach Response Team has been convened, they will be responsible for agreeing and leading the further steps outlined in this procedure, as coordinated by the DPO.

6. Remedial Action

In many cases, it may be possible to act to remedy, contain or mitigate the data breach (remedial action), and the College will take all reasonable steps to this end. Activity to minimise the possible

impact of the data breach will be ongoing, even during the investigation stage. Staff members are required to provide their full and immediate cooperation with any instructions from the DPO in this respect.

Remedial action may include, but is not limited to:

- removing unauthorised access to affected data (in extreme circumstances, this may include action by the IT team without the consent of the relevant staff member);
- contacting unintended recipients to require them to destroy the data and to inform them that to access or utilise the data would constitute an offence;
- seeking duplicate copies of lost data;
- remotely wiping data from affected devices where possible; and
- retaining the services of external specialists, such as cyber security experts.

7. Notification

In some circumstances, particularly where a risk is posed to data subjects because of a data breach, College may have a legal duty to notify certain parties. The decision as to whether notification is required will be made by the DPO and/or Data Breach Response Team, and staff members should not share details of the incident without prior authorisation of the DPO.

8. Data Subjects

Where there is a risk of harm to the affected data subjects, College is required to notify them of the breach and provide reasonable assistance to allow them to mitigate that risk. This assistance may include, for example, advice on identity fraud prevention or access to counselling services. Before notifying data subjects, the DPO/Data Breach Response Team will weigh up the risk of harm versus the distress that may be caused to data subjects, and where notification is necessary, will choose a method of communication which will minimise such distress. For example, where the affected data subject is a student, a member of teaching or student support staff may be selected.

9. Police

Where a data breach has occurred because of criminal action, where proven or suspected, the police will be notified without delay. In such cases, the DPO shall consult directly with the police and all reasonable action will be taken to assist any ensuing investigation.

10. ICO

Where a data breach is considered serious, the College is required to notify the ICO within 72 hours of discovery of the breach. The decision as to whether to notify the ICO will be made by the DPO, although the DPO may wish to seek legal counsel and/or advice from the ICO before reaching this decision. Prior to notifying the ICO of a data breach, the DPO will inform the Group Chief Operating Officer (COO) and Communications Team. The DPO will report the breach directly, following the guidelines set out by the ICO.

11. Third Party Data Controllers

Under certain circumstances, where the College is a Data Processor or Joint Data Controller for the data affected by a data breach, there may be a contractual obligation to notify the relevant Data Controller of the breach. Staff members reporting a breach should inform the DPO if they are aware of a Data Controller or Data Sharing Agreement to which the breach is relevant. Where third party notification is required, the DPO will contact the third party directly and will manage any coordinated response as required.

12. Risk Management

Where a data breach poses a reputational, legal, or financial risk to the business, this risk will be initially assessed by the DPO/Data Breach Response Team, who will also agree recommendations for action to mitigate those risks. Where those risks are considered to be material, the risk assessment and action plan will be subject to the scrutiny and approval of the COO and/or CEO (Chief Executive Officer).

Actions to mitigate organisational risk, as approved by the COO and/or CEO, if necessary, shall be included in the Data Breach Action Plan, and may include:

- seeking and following the advice of the organisation's legal advisors;
- a robust PR and communications plan (to include internal and external communications); and/or
- notifying the insurers of the incident.

Where the organisational risk is considered material, the Group Executive Team will be informed of the incident and the agreed Data Breach Action Plan.

13. Third-Party Breaches

A Third-Party Data Breach occurs when a data breach occurs to a partner of the College, which affects data controlled by the College and/or its stakeholders. The Data Sharing Agreements operated by the College require Data Processors and Joint Data Controllers to inform the DPO without delay in the event of a breach affecting College data, and to provide reasonable assistance in such cases.

Upon being informed of a Third-Party Data Breach, the staff member must immediately notify the DPO of the breach, as outlined in this procedure. The DPO will initiate the action required under this procedure and will consult directly with the third party to agree on how necessary actions will be shared.

14. Follow Up Action

Following the initial response to a data breach, and once any immediate risks are alleviated, the DPO will decide whether any follow-up action is required. This may include additional training for the staff or department(s) involved and/or alterations to relevant systems or processes.

All breaches will be investigated (thoroughness depending on severity of the breach) to identify weaknesses in processes, systems, controls and/or training that allow the data breach to arise. In the more severe cases, the DPO will prepare an investigation report, including recommended actions to address any weaknesses identified. These reports and follow up the Compliance Committee shall monitor actions.

In cases where a data breach occurred because of (suspected or proven) misconduct or negligence by a staff member, the DPO will notify HR and the staff member's line manager of the incident. The HR team will be responsible for ensuring that any necessary investigatory or disciplinary action is undertaken.

15. Reporting

All data breaches and subsequent actions taken under this procedure will be recorded in full on the Data Breach Register. Information from the Register will be regularly reviewed by the DPO and the Compliance & Risk Committee, to identify trends and organisational weaknesses, and to agree recommendations for action. Data breach information will be included in the annual report to the Group Executive Team.

In the event of serious breaches posing a significant risk to the organisation, a report will be issued to the Board of Governors.

Risk Assessment Process for Data Incidents

Once the Data Protection team has been notified of a potential data breach or data incident they will instigate the process, The risk assessment approach is used to identify if a Data Incident meets the criteria to become a Data Breach and the ICO is required to be notified.

1. Firstly, think about the threat events, and likelihood, which could impact the confidentiality, accuracy, or availability of the data you are collecting, processing, or storing.

2. Next assign a numerical value to the **Likelihood**, as listed below:

   5 - Highly Likely - Data has been shared and to numerous recipients

   4 – Likely - Data is likely to be shared and to more than a small number of recipients

   3 - Possible - Data may be shared, but only to a small number of recipients

   2 - Unlikely - Little chance of data being shared

   1 - Highly unlikely - Almost no chance personal data being shared

3. Then consider the **impact** of the event and assign a numerical value as listed below:

   1 - Disclosure of no more than two personal details, from name, address, course name or code, emails, telephone number or date of birth of data subjects.

   2 - Disclosure of more than two personal details i.e. name, address, emails, telephone number, date of birth, of some data subjects.

   3 - Disclosure of several personal details, such as name, address, emails, telephone number, date of birth, undefined medical data, or personal contact of some data subjects.

   4 - Disclosure of personal details, such as name, address, telephone number, emails, date of birth, gender, medical data, bank details, conversations, and any additional data, which could result in small number of data subjects suffering harm, anxiety, or identity theft as a direct result of disclosure.

   5 - Disclosure of personal details, such as name, address, telephone number, emails, date of birth, gender, medical data, bank details, conversations, and any additional data, which could result in many data subjects suffering harm, anxiety, or identity theft as a direct result of disclosure.

4. Multiply the Likelihood value (para 2.) by the Impact value (para 3.) to determine a risk score

   a. Data Breach – If there is a Data Breach then this figure for each event will help decide further action by the DPO and senior staff, for instance if the breach needs reporting to the ICO.

Example

A laptop has been left on unattended in a public place. A member of the public has witnessed a stranger placing a data stick into the computer and thought it likely that data was removed. There was a spreadsheet on the desktop containing names, address, email address, telephone number and some comments of over 50 data subjects but no medical information or bank details

Event	Likelihood	Impact	Risk Result	Comment
Data has been removed from the computer	5	3	5x3=15	Medium / High risk - This is serious enough to be reported to the ICO. This is as much a precaution due to the number of pieces of data stolen rather than the nature of the data. Although the nature of the comments needs to be considered. It is also a breach of policy and data subjects, if known should be contacted.