Title: Data Protection Policy	Ref:CP005	Version:3
Approval Body: Corporation	Date: 21 May 2018	Review Date: 31 July 2021
Lead Person: Clerk to the Corporation		
Equality Impact Assessment: to be completed		
Version:	Reviewer/Approval	Review Notes
1. October 2012	SMT/Policy Group	
2. 24 March 2015	Data Protection Review Group/ Audit & Risk Committee	Full review
3. May 2018	Group Executive Team	Full review

DATA PROTECTION POLICY

Introduction

Activate Learning processes certain personal data about its employees, students and other stakeholders for a variety of defined purposes, such as to allow us to allow access to computer systems and monitor performance, achievements, and health and safety. In order to protect the privacy of our stakeholders, and to comply with the principles laid out in law, information must be collected and used fairly, stored securely and confidentially, and destroyed when it is no longer needed.

Policy Statement

Activate Learning recognises that the correct and lawful treatment of personal data will protect our stakeholders, maintain confidence in the organisation and support successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. Activate Learning could be exposed to fines of up to €20 million (approximately £18 million), depending on the offence, for failure to comply with the provisions of the relevant legislation.

Purpose

The purpose of this policy is to ensure that all staff understand their responsibility to adhere to and comply with the requirements of the data protection legislation. Failure to adhere to this policy, whether regarding another staff member, student or a third party, will be regarded as potential misconduct and may result in disciplinary proceedings being brought.

Scope

This policy applies to all employees, volunteers, students and customers of Activate Learning who process personal data, and covers all personal data we process, regardless of the method of storage or type of data subject. This includes emails, notes and documents containing personal data.

Definitions

Staff: all employees, workers, volunteers, governors and others.

Consent: a freely given, specific, informed and unambiguous indication of a data subject's agreement to the processing of personal data relating to them, given by a clear positive action.

Data Breach: the accidental or unlawful destruction, loss, alteration or unauthorised access, disclosure or acquisition, of personal data.

Data Controller: the person/organisation that determines when, why and how to process personal data. Activate Learning is the Data Controller of all personal data that we process for our own purposes.

Data Owners: Directors responsible for key categories of personal data: Group Director of Institutional Effectiveness (student data), Group Director of HR (staff data), Group Director of Marketing (customers).

Data Processor: an external person or organisation who processes information on our behalf.

Data Sharing Agreement (DSA): a legal agreement or contract outlining data sharing activity and the responsibilities of parties who are sharing data.

Data Subject: a living, identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): a tool to identify and reduce the risks of a data processing.

Data Protection Officer (DPO): the person responsible for providing advice and guidance relating to data protection. The DPO for Activate Learning is the Clerk to the Corporation.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*).

Personal Data: any information which, either on its own or if combined with other information which might reasonably be held by Activate Learning, could uniquely identify a data subject. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion or intention.

Privacy Notices: notices setting out information about the processing of personal data, which must be provided to data subjects when we collect information about them.

Processing or Process: any activity that involves the use of personal data, including obtaining, recording storing, organising, amending, retrieving, using, disclosing, transferring, erasing or destroying it.

Pseudonymisation or Pseudonymised: replacing identifying information with a pseudonym, so that the data subject cannot be identified without the use of information which is kept separately and securely.

Related Policies: Activate Learning's related policies, guidelines and procedures which are provided to assist in implementing this policy, and are available on the Data Protection page of the Staff Portal.

Special Category Data: personal data revealing race or ethnicity, political opinion, religious beliefs, trade union membership, health conditions, sex life, sexual orientation, biometric or genetic data, or criminal offences or convictions.

Responsibilities

The Data Protection Officer is responsible for:

- Overseeing and maintaining this and related policies, procedures and guidance;
- Providing advice and guidance on all aspects of data protection;
- Maintaining central records which evidence Activate Learning's compliance with the relevant legislation, including data maps and registers of DSAs, Privacy Notices and data breaches;
- Ensuring staff receive adequate training to support compliance with the relevant legislation;
- Reviewing contracts and DSAs to ensure legal compliance is assured;
- Coordinating responses to data breaches and exercise of data subject rights, liaising with the Information Commissioner's Office (ICO) as necessary;
- Conducting internal audits and checks of data processing activities and data protection records;
- Monitoring changes to legislation and updating policies, procedures and guidance as necessary.

Data Owners are responsible for:

- Maintaining an overall data map of personal data relating to their data subject group;
- Maintaining and updating privacy notices and ensuring that these are provided to their data subject group as required;
- Maintaining central databases of personal data relating to their data subject group, and ensuring access to those databases is appropriate.

Data Protection Champions are responsible for:

- Promoting good data protection practice in their business areas;
- Supporting the development and maintenance of local data maps, privacy notices and retention schedules;
- Supporting the completion of DPIAs as necessary.

Directors, Managers and Team Leaders are responsible for:

- Ensuring that their team / business area processes reflect 'privacy by design' and incorporate adequate safeguards for personal data;
- Ensuring that DPIAs are undertaken whenever a process is significantly changed or a new process is developed;
- Ensuring that local data maps, privacy notices and retention schedules are kept up to date;
- Ensuring that DSAs or an equivalent contract is in place to cover any external data sharing;
- Ensuring that their teams are aware of and comply with this and related policies.

All staff are responsible for:

- Complying completely with this and related policies;
- Ensuring that they have an awareness of the purpose and legal basis for all personal data processing they undertake;
- Following local and central retention schedules;
- Adhering to the limitations of the Privacy Notices and DSAs in place;
- Notifying the relevant person if a change is required to a Privacy Notice, data map, or DSA;
- Ensuring all personal data storage is adequately secure;
- Promptly notifying the DPO of data breaches and requests to exercise any data subject right.

Data Protection Principles

We adhere to the principles relating to processing of personal data set out in the GDPR which require personal data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

(b) Collected only for specified, explicit and legitimate purposes, and used only for these or compatible purposes (Purpose Limitation);

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation);

(d) Accurate and where necessary kept up to date (Accuracy);

(e) Not kept for longer than is necessary for the purposes for which the data is processed (Storage Limitation);

(f) Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage (Security, Integrity and Confidentiality);

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation);

(h) Made available for data subjects to exercise certain rights in relation to their personal data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

Lawfulness, Fairness and Transparency

Lawfulness and Fairness

The GDPR restricts our processing of personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly. The GDPR allows processing for specific purposes, some of which are set out below:

(a) the data subject has given his or her **consent**;

(b) the processing is necessary for the performance of a **contract** with the data subject;

(c) the processing is necessary and proportionate for the fulfilment of our tasks as a public authority in the **public interest**;

(d) to meet our **legal obligations**;

(e) to protect the data subject's **vital interests**; or

(f) to pursue our **legitimate interests** for purposes where they are not overridden by the interests or fundamental rights and freedoms of data subjects. This purpose only applies to activity that is not part of our tasks as a public authority.

You must understand the legal grounds being relied on for each processing activity. This will be set out in your department's data map or the central data map. If the data you are processing or the purpose for which you are processing it is not captured on the data map, you must notify your line manager immediately. Further guidance on the completion and maintenance of data maps is available in the **Data Mapping Guidance Note** on the Data Protection page of the staff portal.

Special Category Data

Under GDPR, in order to process Special Category data, we must identify which of the legal grounds listed above we are processing it under, as well as identifying which of the secondary, Article 9 grounds we are processing it under. The Article 9 grounds for processing are as follows:

(a) the data subject has given explicit consent;

(b) processing is necessary in the context of employment, social security, or social protection law;

(c) processing is required for the purpose of medical treatment undertaken by health professionals;

(d) processing is necessary for reasons of public interest in the area of public health;

(e) processing is necessary for archiving, historical, scientific, research or statistical purposes;

(f) processing is proportionate and necessary for reasons of substantial public interest;

(g) processing is necessary to protect the vital interests of the data subject (or another person) where the data subject is incapable of giving consent;

(h) processing is part of the legitimate activities of a charity or not-for-profit body, with respect to its members or persons with whom it has regular contact in connection with its purposes;

(i) processing relates to personal data which have been manifestly made public by the data subject;

(j) processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity.

When processing Special Category data, you must understand the Article 9 grounds being relied on for each processing activity, as set out in your department's data map or the central data map. If you are unsure, you must clarify the grounds with your line manager or the DPO before processing the data.

Consent

If you are relying upon Consent as your legal grounds for processing personal data you must be sure that valid consent has been obtained from the data subject. When you collect consent, you must keep specific records of the time, date, method and nature of the consent, in line with the **Obtaining and Recording Consent Procedure**, available on the Data Protection page of the Staff Portal. Processing

personal data on the grounds of Consent without ascertaining that valid consent has been obtained is a disciplinary offence.

Valid Consent requires a clear indication of agreement, by way of either a statement or positive action. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are insufficient. Data subjects must be made fully aware of the processing they are consenting to, and consent cannot be required as a condition of service.

Data subjects must be easily able to withdraw consent at any time and withdrawal must be promptly honoured. New consent must be obtained if you intend to process personal data for a different and incompatible purpose to that to which the data subject first consented.

If Explicit Consent is to be relied upon for the processing of Special Category data, this consent must be in written form and attached to a Privacy Notice which clearly outlines the intended processing.

Privacy Notices (Transparency)
Data subjects have the right to be informed of how we are processing their personal data, and therefore the GDPR requires Data Controllers to provide detailed, specific information to data subjects. Activate Learning provide this information through Privacy Notices, which are issued to data subjects upon collection of their data. These Privacy Notices outline how and why we will use, process, disclose, protect and retain the data subjects' personal data, and identifies the Data Controller and DPO.

Privacy Notices for our main groups of data subjects (students, staff and customers) are reviewed and updated by the Data Owners. However, if you are collecting personal data from data subjects who are not covered by these notices or for purposes not covered by the main Privacy Notice, you must use a specific Privacy Notice. All Privacy Notices must be drafted using an Activate Learning template and must be approved by the DPO prior to issue. More information about Privacy notices may be found in the **Privacy Notice Guidance Note** on the Data Protection page of the Staff Portal. Failure to issue a suitable Privacy Notice when collecting personal data is a disciplinary offence.

When personal data is collected via a third party Data Processor, you must check that the personal data was collected in accordance with the GDPR and that an appropriate Privacy Notice, identifying Activate Learning as the Data Controller was issued on collection. It may be necessary to issue a new Privacy Notice to data subjects upon receipt of the personal data.

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes (as set out in the data map and Privacy Notice) and you cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained, unless you have informed the data subject of the new purposes and they have consented where necessary.

Data Minimisation

You must only collect personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You may only collect and process personal data if performance of your duties requires it.

The majority of personal data held and processed by Activate Learning is held on central databases such as REMS, ProMonitor and iTrent. These central databases are managed by the Data Owners in line with Activate Learning policies and procedures and staff should ensure that they make full use of

these databases. You must only take local copies of data contained on these databases when it is necessary for a particular task, and you must delete local copies when they are no longer necessary. In particular, you must be sure not to make or store local copies of Special Category data unless it is absolutely necessary for your duties, and it must be deleted as soon as it is no longer necessary.

Accuracy

Personal data must be accurate and kept up to date. Erroneous data must be corrected or deleted without delay. You must take all reasonable steps to ensure that the data you collect and process is accurate and up to date, including checking the accuracy at point of collection and at reasonable intervals afterwards. Data subjects have the right to request that errors in the personal data we hold on them be rectified, and you should comply with such requests promptly and in line with the **Exercise of Rights Procedure**, found on the Data Protection page of the Staff Portal.

Storage Limitation

Personal Data must not be kept for longer than is necessary for the purposes for which the data is processed, including for the purpose of satisfying any legal, accounting or reporting requirements.

Activate Learning maintains a central Data Retention Procedure and Schedule, and each department or business area is required to maintain a local Retention Schedule which outlines the time for which personal data may be stored. You must ensure that you delete personal data in line with both the central and your local Retention Schedule, taking all reasonable steps to destroy or erase from all storage systems, including paper and electronic copies. This includes erasure of emails containing personal data and requiring third parties to delete such data where applicable.

Failure to erase or destroy personal data in line with central and local Retention Schedules is a disciplinary offence.

Security integrity and confidentiality

Protecting Personal Data
Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Activate Learning develop, implement and maintain appropriate safeguards and regularly evaluate and test the effectiveness of those safeguards to ensure security of our personal data. All staff are responsible for protecting the personal data we hold. You must ensure that reasonable and appropriate security measures are in place for all personal data that you store and process, and you must exercise particular care in protecting Special Category data.

You must maintain data security by protecting the confidentiality, integrity and availability of personal data that you hold and process, defined as follows:

(a) **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.

(b) **Integrity** means that personal data is accurate and fit for the purpose for which it is processed.

(c) **Availability** means that authorised users are able to access the personal data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data. Further information on secure data storage is available in the **Data Storage Guidance Note**, available on the Data Protection page of the Staff Portal.

Secure Data Sharing

You may only share the personal data we hold with another employee of the Activate Learning group if the recipient has a job-related need for the information. In such cases, the personal data should be shared in an appropriately secure fashion, taking into account the sensitivity of the personal data, and in line with the Data Transfer Guidance Note available on the Data Protection page of the Staff Portal.

Activate Learning will only share personal data with third parties where appropriate safeguards and contractual arrangements have been put in place. You may only share personal data with third parties, such as our service providers if:

(a) data sharing is necessary for the provision of contracted services, the furtherance of legitimate Activate Learning purposes, or the fulfilment of a legal or public duty by another public authority;

(b) data sharing complies with the Privacy Notice provided to the data subject and, if required, the data subject's consent has been obtained;

(c) the third party has agreed to comply with the required security standards, policies and procedures;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a Data Sharing Agreement (DSA) or written contract containing approved GDPR clauses is in place. A register of DSAs and approved contracts is available on the Data Protection page of the Staff Portal, and you must check this register before sharing personal data with a third party.

Sharing personal data with a third party without ensuring that all the above criteria are met is a disciplinary offence.

Upon receipt of a new third party data sharing request, you should ask the requester to complete a Data Sharing Request Form, and thereafter you must follow the guidance set out in the **Data Sharing Guidance Note**. These documents are available on the Data Protection page of the Staff Portal and copies of completed forms and signed DSAs or contracts must be provided to the DPO for record-keeping purposes.

Reporting a Personal Data Breach

Activate Learning are required to report certain Data Breaches to the ICO within 72 hours of the Breach being detected, and, in certain instances, to notify the data subject(s) affected.

If you know or suspect that a Data Breach has occurred, do not attempt to investigate or conceal the matter yourself; you must immediately contact the DPO. You should preserve all evidence relating to the potential Data Breach and follow the guidance set out in the **Data Breach Procedure**, available on the Data Protection page of the Staff Portal.

Failure to report an actual or suspected Data Breach is a disciplinary offence.

Transfer Limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. Personal data is transferred across borders when personal data originating in one country is transmitted, sent, viewed or accessed in or to a different country. You may only transfer personal data outside the EEA with the express approval of the DPO and if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country ensures an adequate level of protection for the data subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO; or

(c) the data subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks.

The transfer of personal data outside of the EEA without the express approval of the DPO is a disciplinary offence.

Data Subject's Rights and Requests

Data subjects have rights when it comes to how we handle their personal data. These include rights to:

(a) be **informed** of what of their personal data we process, how and for what purpose(s);

(b) request **access** to their personal data that we hold;

(c) ask us to **erase** their personal data if it is no longer necessary for the purposes for which it was collected;

(d) ask us to **rectify** inaccurate data or to complete incomplete data;

(e) temporarily **restrict** processing of their data in specific circumstances;

(f) **object** to processing justified on the basis of legitimate interests or in the public interest;

(g) ask to receive or for their personal data to be transferred to a third party in a **portable**, structured, commonly used and machine readable format;

(h) object to decisions based solely on Automated Processing;

(i) be notified of a Data Breach which is likely to result in high risk to their rights and freedoms;

(j) prevent our use of their personal data for direct marketing purposes;

(k) withdraw consent to processing at any time;

(l) request a copy of an agreement under which personal data is transferred outside of the EEA; and

(m) make a complaint to the supervisory authority.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation). You

must immediately notify the DPO of any Exercise of Rights request you receive and proceed in line with the **Exercise of Rights Procedure** available on the Data Protection page of the Staff Portal.

Failure to promptly notify the DPO of an Exercise of Rights request is a disciplinary offence.

Privacy By Design and Data Protection Impact Assessment (DPIA)

Activate Learning are required to implement 'Privacy by Design' measures when processing personal data by implementing appropriate technical and organisational measures to ensure compliance with data privacy principles.

All processes involving personal data must take into account Privacy by Design, to ensure that all appropriate measures to protect the personal data are implemented. You are required to conduct a DPIA in respect of all high risk personal data processing and any new process which involves the processing of personal data.

You must use the **Data Protection Impact Assessment Template** and refer to the **DPIA Procedure**, both available on the Data Protection page of the Staff Portal. Completed DPIAs should be shared with the DPO for record keeping purposes.

Automated Processing and Automated Decision-Making

Automated processing occurs when personal data is used to automatically evaluate personal characteristics, in particular to analyse or predict aspects of that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing. A DPIA must be conducted on any automated processing activities.

Automated decision-making occurs when a decision is made which is based solely on automated processing which significantly affects an individual. Automated decision-making is prohibited by law unless:

(a) a data subject has explicitly consented;

(b) the processing is authorised by law; or

(c) the processing is necessary for entering into or fulfilling contract.

Activate Learning do not routinely undertake automatic decision-making. If you intend to make use of automatic processing, you must conduct a DPIA and seek the explicit approval of the DPO before proceeding. Data subjects have the right to be informed of any automated decision-making affecting them, and their right to object to this.

It is a disciplinary offence to undertake automated decision-making in respect of any data subject without the prior approval of the DPO.

Direct Marketing

Activate Learning are subject to certain rules and privacy laws when marketing to our customers. In particular, the data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). There are some limited exceptions to this rule, which are outlined in the relevant guidance note. All direct marketing materials should clearly and explicitly offer the opportunity

to object to direct marketing, and a data subject's objection to direct marketing must be promptly honoured.

When undertaking direct marketing activities, you must inform the DPO of these activities and follow the guidance set out in the Direct Marketing Guidance Note, available on the Data Protection page of the Staff Portal.

Undertaking direct marketing activity without informing the DPO and failure to follow the guidelines set out for direct marketing are disciplinary offences.

Freedom of Information and Publication of Information

Activate Learning is classed as a Public Authority under the Freedom of Information Act 2000. As a result, we are obliged to make certain information public and respond to Freedom of Information requests. The information to be disclosed and/or published in line with this legislation will not include personally identifiable information.
In order to comply with this legislation, Activate Learning has a Freedom of Information Publication Scheme available on our website. However, in addition to this certain personal data will be available to the public for inspection:

- Names of governors;
- Register of interests of Governing Body members and senior staff with significant financial responsibilities;
- Names, job roles and contact details of key staff.

If you fall into one of these categories, and have reason to object to your information being published in this manner, please contact the DPO immediately.

If you receive a Freedom of Information request, you must refer it to the DPO immediately, in line with the **Freedom of Information Procedure**, available on the Data Protection page of the Staff Portal. You must not attempt to answer a request directly.

Record Keeping

Under GDPR Activate Learning are required to keep full and accurate records of all our data processing activities. You are responsible for helping us to maintain these records by ensuring that the following documents are up to date, accurate and shared with the DPO:

(d) Data Maps;

(e) Retention Schedules;

(f) Privacy Notices;

(g) Data Sharing Agreements (or contracts with adequate GDPR clauses);

(h) DPIAs.

If you are collecting and relying upon Consent for your processing activities, you must keep and maintain accurate records, in line with the **Obtaining and Recording Consent Procedure**, available on the Data Protection page of the Staff Portal.

Training and Audit

We are required to ensure all staff have undergone adequate training to enable them to comply with data privacy laws. This training will include mandatory Activate Learning Online training for all staff and workshops and refreshers for staff with particular responsibilities around data protection. You must ensure that you complete the training required for your job role, and inform the DPO if a new member of staff joins your team and requires data protection training.

Activate Learning have established a Data Protection Champion scheme, which ensures that key members of staff in each business area receive additional and ongoing training to support data protection best practice in their areas. If your business area does not have a Data Protection Champion, or your Data Protection Champion leaves, you must inform the DPO immediately.

We must also regularly test our systems and processes to assess compliance. You must regularly review all the systems and processes under your control to ensure they comply with this and related policies, and check that adequate controls and resources are in place to ensure proper use and protection of personal data.

Internal data protection audits will be undertaken periodically to ensure that adequate measures are in place to protect personal data. You are required to comply with these audits and action any recommendations which arise from them.

Changes to this Privacy Standard

This Data Protection Policy will be subject to regular review and update, so please check back regularly to obtain the latest copy.