



TITLE	REF	VERSION
Exercise of Rights Procedure	GOVPRO009	2.1

  

DEPARTMENT	Governance		
DATE	11 May 2020	REVIEW DATE	11 May 2021

## EXERCISE OF RIGHTS PROCEDURE

### Procedure Statement

Activate Learning processes certain personal data about its employees, students and other stakeholders for a variety of defined purposes. The people about whom we hold and process data (the Data Subjects) have certain rights in respect of their personal data, which Activate Learning, as the Data Controller, are required to comply with. This document outlines the procedure for receiving and responding to requests from data subjects to exercise any of these rights.

All staff of Activate Learning are required to recognise and respond appropriately to an exercise of rights request, and should therefore familiarise themselves with this procedure.

### Definitions

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

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

**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 Protection Officer (DPO):** the person responsible for providing advice and guidance relating to data protection. The DPO for Activate Learning is the Director of Governance.

**Data Protection Legislation:** includes the Data Protection Act (DPA) (UK - 23 May 2018), the General Data Protection Regulation (GDPR) ((EU) 2016/679), and other such legislation as governs data protection in the UK.

**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.

**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.

### Rights of the Data Subject

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

- ask us to rectify inaccurate data or to complete incomplete data – this may include requests to correct or update information such as contact details, educational or employment records, or personal information;
- withdraw consent to processing at any time – this right applies to processing that is undertaken on the basis of consent, such as the storage and publication of photographs, or direct marketing activity;
- be informed of what of their personal data we process, how and for what purpose(s) – this right is normally fulfilled through the issue of Privacy Notices, but may be specifically requested at any time;
- request access to their personal data that we hold – this may include requests to view or receive copies of any or all of their information, records, files etc. Requests to exercise this right may or may not be specifically referred to as Subject Access Requests;
- ask us to erase their personal data if it is no longer necessary for the purposes for which it was collected – this may also be referred to as the right to be forgotten, and may include requests for us to delete or destroy some or all of the information and/or records we hold about someone.

- 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 – this may include students requesting for their educational records to be transferred to another school or college.
- object to direct marketing or processing justified on the basis of legitimate interests or public task – this may occur if the data subject perceives that the processing may cause them harm; and
- temporarily restrict processing of their data in specific circumstances – this will most likely be in the case of legal disputes, where processing may be temporarily prevented until the matter is resolved.

In addition to these rights, data subjects also have the rights to:

- object to decisions based solely on Automated Processing – Activate Learning do not undertake any Automated Processing activity;
- be notified of a Data Breach which is likely to result in high risk to their rights and freedoms – this will happen through the Data Breach Procedure;
- request a copy of an agreement under which personal data is transferred outside of the EEA – Activate Learning do not routinely transfer personal data outside of the EEA, and will seek the data subject's explicit consent before doing so; and
- make a complaint to the supervisory authority – the data subject is required to contact the supervisory authority (in the UK, the ICO) directly.

Under normal circumstances, Activate Learning is not expected to receive requests relating to these additional rights. Therefore, these rights are not specifically covered in this procedure, however any requests relating to these rights should be immediately referred to the DPO.

### **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 Activate Learning 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:

#### **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 Activate Learning 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.

#### **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.

#### **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.

#### **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. Activate Learning are 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.

### **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:

#### **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.

#### **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 (if applicable).

#### **Confirming the Request**

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

### **Identifying Relevant Data Sets**

In order 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:

<b>For students:</b>	Institutional Effectiveness Group Administration Admissions / Student Support Learner Support Relevant Faculty/ies IT Marketing
<b>For staff:</b>	HR Relevant Department/Team ALF (for teachers) IT
<b>For business contacts:</b>	Relevant Faculty / Department Marketing Career Pathways Directors
<b>For customers:</b>	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.

### **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 Activate Learning may reasonably hold, could uniquely identify the data subject. This will include any correspondence, documents or notes that make reference 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 Activate Learning breaching its obligations under data protection law, and therefore may be a disciplinary offence.

## **Procedures for Specific Types of Request**

### **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.

### **Withdrawal of Consent**

Where personal data is processed on the basis of 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 Activate Learning 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.

### **Subject Access Requests**

In order to process a Subject Access Request, the DPO's office will contact the relevant departments (or in some cases, all Activate Learning Staff) to request that they supply copies of any and 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 timeframe.

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.

### **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, in the event that 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.

### **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.

In the event that 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.

In the event that the right to data portability does apply, the DPO's office will contact the relevant departments to seek electronic copies of the relevant 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 and will expire within two weeks.

### **Objection Requests**

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

#### *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.

#### *Public Task or Legitimate Interest*

Where a data subject objects to processing of their personal data which is undertaken on the basis of 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 Activate Learning's legitimate reasons for processing the data with any risk or harm to the data subject. In order 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.

### **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.

### **Administration and Response to a Request**

Activate Learning 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 a number of 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 likely 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 on the basis of 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, in the event that 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.

### **References**

This Policy complies with the following legislation:

- [Data Protection Act 2018](#)
- [General Data Protection Regulation 2018](#)

This Policy should be read in conjunction with the following Activate Learning Policies and Procedures:

- Information Security and Data Protection Policy

