TITLE	REF	VERSION
Data Breach Procedure	GOVPRO008	2.1

DEPARTMENT	Governance		
DATE	09 December 2019	REVIEW DATE	19 April 2023

DATA BREACH PROCEDURE

Procedure Statement

Activate Learning processes certain personal data about its employees, students and other stakeholders for a variety of defined purposes, and has a responsibility to adequately protect that data. In the event that the security of personal data processed by Activate Learning 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.

Definitions

Staff: all employees, workers, volunteers, governors and other stakeholders.

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 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 Legislation: includes the General Data Protection Regulation (GDPR) (EU) 2016/679), the Data Protection Act (2018) and other legislation relating to data protection in force at the point of application.

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.

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

ICO: Information Commissioner's Office, the regulatory authority responsible for enforcing the relevant Data Protection Legislation.

Joint Data Controller: any person/organisation with whom Activate Learning shares data controller rights in respect of certain personal data.

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.

Scope

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

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 as a result 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 possible 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 Data Breach Notification form on the Staff Portal, or, if the breach is serious or urgent, by calling the DPO's office on 01865 551228. In some cases, the staff member who reported the breach may be required to assist in gathering further information to assist DPO's investigation and response.

Investigating A Data Breach

Upon notification of a breach, 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.

So as 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, so as to minimise the impact and risk to the data subjects and Activate Learning.

Risk Assessment

Once sufficient information has been gathered, the DPO will conduct a risk assessment of the breach, which will take into account 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.

On the basis of 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.

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, which may include:

- Group Director for Institutional Effectiveness;
- Group Director for IT and Digital Education;
- Group Director for People and Change;
- Group Director for Student Services;
- Group Director for Property and Facilities; and
- Group Executive Director for the affected faculty or division.

The DPO will contact each Director required in the particular 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 Officer, the PR and Communications Manager, or the Facilities 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.

Remedial Action

In many cases, it may be possible to take action to remedy, contain or mitigate the data breach (remedial action), and Activate Learning will take any and 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.

Notification

In some circumstances, particularly where a risk is posed to data subjects as a result of a data breach, Activate Learning 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.

Data Subjects

Where there is a risk of harm to the affected data subjects, Activate Learning are 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 reasonably minimise such distress. For example, where the affected data subject is a student, a member of teaching or student support staff may be selected.

Police

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

ICO

Where a data breach is considered serious, Activate Learning are required to notify the ICO within 72 hours of discovery of the breach. The decision as to whether or not 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 Financial Officer (CFO) and Communications Team. The DPO will report the breach directly, following the guidelines set out by the ICO.

Third Party Data Controllers

Under certain circumstances, where Activate Learning 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.

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 CFO and/or CEO.

Actions to mitigate organisational risk, as approved by the CFO 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.

Third-Party Breaches

A Third-Party Data Breach occurs when a data breach occurs to a partner of Activate Learning, which affects data controlled by Activate Learning and/or its stakeholders. The Data Sharing Agreements operated by Activate Learning require Data Processors and Joint Data Controllers to inform the DPO without delay in the event of a breach affecting Activate Learning 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 liaise directly with the third party to agree how necessary actions will be shared.

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.

In the case of serious breaches, a thorough investigation will be conducted to identify weaknesses in processes, systems, controls and/or training that allowed the data breach to arise. In such cases, the DPO will prepare an investigation report, including recommended actions to address any weaknesses identified. These reports and follow up actions shall be monitored by the Data Protection Committee.

In cases where a data breach occurred as a result 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.

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 Data Protection Committee, so as 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.

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