Data Breach Policy

DP/04

Date issued:	August 2023
Date reviewed:	September 2025
Author:	Data Protection Officer
Policy Owner:	Company Secretary
Next review date:	September 2027

Advance HE
Equality, Diversity, and Inclusion Statement

Advance HE's charitable objects illustrate our clear commitment to advancing equality, diversity, and inclusion (EDI). Encouraging EDI in the workplace as a core organisational value, underpinning internal practice in order for people to feel welcome valued and supported.

At Advance HE, we are committed to creating an environment free of bullying, harassment, victimisation, and unlawful discrimination, promoting dignity, and a safe, inclusive, and respectful environment. We are committed to ensuring that all stakeholders are treated fairly and are not subject to discrimination on any grounds.

CONTENTS

APPENDICES

Advance HE
Data Breach Policy

1 Purpose

1.1 Advance HE is committed to ensuring that the business activities which involves the use of personal data are in line with the UK Data Protection Act 2018, the Data Use and Access Bill and the Privacy and Electronic Communications Regulations, known collectively as "UK Data Protection Legislation".

1.2 Advance HE is obligated under the Data Protection legislation to have in place a security framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

1.3 Advance HE collects, holds, processes and shares personal data and it ensures that it will take every care to protect personal data from incidents (either accidental or deliberate) that could lead to a data protection breach.

1.4 Compromise of information, confidentiality, integrity or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance and/or financial costs.

2 Scope

2.1 This Policy sets out the procedure to be followed in the event that a data breach occurs to ensure a consistent and effective approach when managing a data breach and information security incidents across Advance HE.

2.2 This Policy has been developed to contain data breaches, to mitigate or minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

2.3 This Policy applies to all colleagues at Advance HE. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of, Advance HE.

3 Definitions

Term	Definition
Personal Data	Information relating to an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier. This Policy relates to all personal and special category (sensitive) data held by Advance HE. This also includes any personal data which "relates to" an individual.
Data Breach	For the purpose of this policy, data security breaches include both confirmed and suspected incidents, and breaches that are accidental or deliberate as well as near misses. The Data Protection Act 2018 defines a personal data breach as: '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*'.
Data Subject	All living individuals about whom Advance HE holds personal data.

Colleagues	All persons working for Advance HE or on its behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, associates, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with Advance HE.
Processing	Any activity that involves the use of personal data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.
Near Miss	An incident that had the potential to result in a personal data breach but was prevented or mitigated before any actual breach occurred.
Reasonable Interval	This relates to the timeframe a data subject makes another request and whether there have been any changes to the data in the request.
Relates To	This is data that identifies an individual, even where a name is not present, where the content is obviously relating or links to the individual.
E-Commerce	Exchange of personal data over the internet.
Data Controller	The individual or organisation which control and determine, subject to the permission given to them by the law or the data subject, how and why any personal information is processed.
Data Processor	Individuals / organisations who processes personal information on behalf of a data controller. Colleagues are excluded from this definition.

4 Roles and Responsibilities

4.1 The **Data Protection Officer** has the overall responsibility for reviewing and assessing data breaches. They have the following responsibilities under this Policy:

- Review, assess and investigate data breaches.
- Implement recovery action plans following a breach.
- Liaise with key departments to obtain the relevant information for data breaches.
- Maintain a data breach log and report on breaches and trends to the Audit, Finance and Risk Committee.
- Liaise with any parties who may be affected by the data breach, including data subjects and data controllers.
- Report relevant data breaches to the Information Commissioner and support their investigation.
- Implement any action plans advised by the Information Commissioner.
- Provide training and guidance on data breaches, and prevention of data breaches to colleagues.
- Notify authorities as appropriate in the event of a data breach, such as Police, Charity Commissions, and ActionFraud.

4.2 The **IT Team** have the following responsibilities under this Policy:

- Investigate any security breach on systems should the data breach involve security incidents.
- Notify the Data Protection Officer on any potential or confirmed security breach.
- Implement a recovery plan to ensure security systems are back up and running.

- Maintain technical and organisational measures on Advance HE systems.
- Provide training and guidance on cyber security, Advance HE security measures and prevention of security breaches.

4.3 All **colleagues** have the following responsibilities under this Policy:

- Immediately report any potential or confirmed data breach to the Data Protection Officer.
- Support the Data Protection Officer in completing the data breach investigation.
- Ensure any data held and systems used remains up-to-date, accurate and in line with the security measures and systems.
- Follow Data Protection and IT security policies.

5 Data Breach

5.1 A personal data breach may, depending on the circumstances, concern the confidentiality, integrity and availability of personal data or any combination of these.

- **Confidentiality** – Unauthorised or accidental disclosure of, or access to, personal data.
- **Integrity** – Unauthorised or accidental alteration of personal data.
- **Availability** – Accidental or unauthorised loss of access to, or destruction of, personal data.

5.2 A personal data breach includes, but is not limited to, the following:

- Loss or theft of confidential or sensitive data.
- Loss or theft of equipment which data is stored.
- Equipment or data information systems failure.
- Unauthorised use of, access to or modification of data or information systems.
- Attempts (failed or successful) to gain unauthorised access to data information systems or Advance HE's security systems.
- Unauthorised disclosure of, or access to, sensitive / confidential data.
- Website defacement.
- Hacking, phishing or malicious attacks.
- Unforeseen disruptive incident which impacts the integrity or confidentiality of personal data.
- Human error, such as incorrection alteration or erroneous mailing.
- Fraud attacks, such as information is obtained by deceiving Advance HE.
- Unauthorised access to personal data from third party.
- Colleagues without authorisation rights accessing personal data.
- Data corruption due to IT system errors.
- Malicious tampering with stored data.
- Incorrect deletion of data without suitable back-up systems.

5.3 A personal data breach can have significant adverse effects on data subjects, which may result in physical, material or non-material damage. This may include:

- Loss of control over their personal data.
- Limitation of their data subject rights.
- Discrimination.

- Identity theft or fraud attacks.
- Financial loss, including Information Commissioner fines or data subject compensation.
- Unauthorised reversal of pseudonymisation.
- Damage to reputation.
- Loss of confidentiality of personal data protected by professional secrecy or required to protect the individual from physical danger.
- Significant economic or social disadvantage to individuals.

Procedures

6 Reporting a Data Breach

6.1 Colleagues who access, uses or manages information held or processed by Advance HE is responsible for reporting a data breach and information security incidents immediately when they become aware of the breach to the Data Protection Officer on data.protection@advance-he.ac.uk.

6.1.1 In the event that the investigation identifies a colleague has maliciously caused a breach to data protection legislation, Advance HE will implement the Disciplinary Policy and potential legal action.

6.2 When reporting a breach, colleagues are required to complete the data breach form found in appendix A. This provides the Data Protection Officer with key information on the data breach to allow for effective assessment and recovery plans.

7 Investigating A Data Breach

7.1 Upon receipt of a completed Data Breach Form, the Data Protection Officer will firstly determine whether the breach still ongoing. If so, the Data Protection Officer will identify appropriate steps which are to be taken immediately to minimise the effect of the breach.

7.2 An initial assessment will be undertaken by the Data Protection Officer in liaison with relevant Team, such as the IT Team or the People Team, to establish the severity of the breach.

7.2.1 Should the Data Protection Officer identify that there was a security breach to Advance HE's systems, they will notify the IT Team immediately who will be responsible for investigating the system breach and implementing recovery measures.

7.2.2 The Data Protection Officer may be required to seek advice from experts in order to resolve the breach promptly.

7.3 An investigation will be undertaken by the Data Protection Officer immediately and, wherever possible, within 24 hours of the breach being discovered / reported. The investigation will consider:

- The type of personal data involved and its sensitivity.
- The prevention measures in place which mitigated the impact of the breach.
- The event which caused the data breach.
- Whether the personal data could be used for any illegal or inappropriate use.
- Data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s).

- Whether there are wider consequences to the breach.
- Any third parties are required to be notified, including the Data Subject, Data Controllers, Information Commissioner, Police or any other regulatory authority.

7.4 The Data Protection Officer will establish whether there are any actions required to recover any losses and limit the damage the breach could cause. The Data Protection Officer will determine the suitable course of action to be taken to ensure a resolution to the incident and notify the relevant colleagues to implement the recovery action plan.

7.5 Colleagues must act immediately on any instructions given by the Data Protection Officer and/or IT Team. Failure to implement the recovery action plans may lead to disciplinary action.

7.6 Once the initial incident is contained, the Data Protection Officer with support from the IT Team will carry out a review of the causes of the breach; the effectiveness of the response; and whether any changes to systems, policies and procedures should be undertaken. The review will consider:

- Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.
- Where and how personal data is held and where and how it is stored.
- Where the risks lie, including identifying potential weak points within existing security measures.
- Whether methods of transmission are secure; sharing minimum amount of data necessary.
- Staff awareness and training.

7.7 If deemed necessary, a report recommending any changes to systems, policies and procedures will be reviewed by the Chief Executive Group.

7.8 All data breaches should be logged in the Advance HE Data Breach Register accompanied with the evidence and investigation outcomes which are held for legal and audit purposes.

8 Notification

8.1 In the case of a personal data breach with result in a risk to the rights and freedoms of data subjects, the Data Protection Officer will, without undue delay, shall notify breach to the Information Commissioner no later than 72 hours after having become aware of it.

8.1.1 Where the notification to the Information Commissioner is not made within 72 hours, the Data Protection Officer must provide reasons for the delay. The Data Protection Officer will support the Information Commissioner in assessing the data breach, and any actions plans implemented.

8.2 The Data Protection Officer may be required to notify third parties such as the police, insurers, banks or credit card companies and trade unions, in cases where illegal activity is known or is believed to have occurred or where there is a risk that illegal activity might occur in the future.

8.3 Where the data breach has a significant impact on the public, the Data Protection Officer will liaise with the Marketing and Communications Team to arrange for a press release and to handle any incoming press enquiries.

8.4 Under the Data Protection legislation should the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, Advance HE is required notify communicate the personal data breach to the data subject without undue delay.

8.5 The Data Protection Officer will provide specific information to the Data Subjects regarding the data breach and additional measures they should take to protect themselves from any negative consequences which may result from a data breach.

9 Regional Variation

9.1 Advance HE operates in various countries, whom have their own Data Protection legislation. However due to the processing of data taking place within the UK, Advance HE will ensure that all data subjects, no matter where they are from, is subject to the same data subject rights as per this Policy.

9.2 Advance HE, where appropriate, will also consider and identify any additional factors from in-country Data Protection legislation should there be data processed within that country.

10 Additional Information

10.1 Advance HE reserves the right at any time to make any variations to and to amend this Policy and any other Associated Policy as it sees fit.

10.2 If any variation or amendment has taken place, a notification of the updated Policy shall be sent to all colleagues. It is the colleague's responsibility to ensure they adhere to the correct and current version.

Appendix A: Data Breach Form

This form has been created for colleagues to complete when they have breached data protection practices or become aware of a data breach.

Once completed, please send to the Data Protection Office at data.protection@advance-he.ac.uk as soon as possible.

For further support on Data Protection practices, please refer to the Data Protection Services Internal Guidance.

***Date:**	

Contact Details for Responsible Persons

Data Protection Officer	
Name	Becky Hamer
Email Address	Data.protection@advance-he.ac.uk
Department	Corporate Support

***Responsible Person for Data Breach**	
Name	
Email Address	
Department	

Information on the Data Breach

***Date of Breach**	
***Time of Breach**	
***Processing Activity**	
***How did you become aware of the breach?**	
***Is the incident ongoing?**	Yes ☐ No ☐

***Type of Data Breach**		
☐ Cyber Attack	☐ Ransomware	☐ Malware
☐ Phishing	☐ Software Error	☐ Skimming
☐ Theft	☐ Loss	☐ Erroneous Mailing
☐ Wrong Disposal	☐ Incorrect Erasure	☐ Other: Click here to insert text
☐ Inaccessible Data	☐ Incorrect Alteration	
☐ Improper disclosure	☐ Unauthorised Access	

***Description of Data Breach**

***Categories of Data Affected by the Breach:**

☐ Name / Identification Information ☐ Health ☐ Economic Situation ☐ Religious / Philosophical beliefs ☐ Trade Union Membership ☐ Confidential Work Documentation ☐ Location ☐ Email Addresses ☐ Password ☐ Learner Behaviour ☐ Disabilities ☐ Identity Documents	☐ Date of Birth ☐ Banking/ Finance ☐ Sex Life or Sexual Orientation ☐ Political Opinions ☐ Biometric Data ☐ Photos / Videos ☐ Mailing Addresses ☐ Information on Criminal Convictions ☐ Identifying Factors (Pseudonymised Data) ☐ Employment Details ☐ Other: Click here to insert text

***Number of Affected Data Subjects**	

***Categories of Data Affected Data Subjects**	
☐ Employees ☐ Customers ☐ Clients ☐ Child / Minors ☐ Associates ☐ Other: Click here to insert text	☐ Users ☐ Potential Customers ☐ Members of the Public ☐ Service Providers
***Has the Data Subjects been Notified?**	Yes ☐ No ☐

***Origin of the Affected Personal Data**
Please detail how you came about the personal data, and why Advance HE was processing the data.

***Remedial Measures**		
Action	**Who completed the action?**	**When was the action completed?**

Potential Consequences of Data Breach:	
☐ Discrimination ☐ Identify Theft / Fraud ☐ Life Hazard ☐ Financial Damage ☐ Economic Disadvantages ☐ Unauthorised Reversal of Pseudonymisation	☐ Job Loss ☐ Loss of Confidentiality (protected by professional secrecy) ☐ Reputational Damage ☐ Social Disadvantages ☐ Physical Threats ☐ Other: Click here to insert text

Notifications on the Data Breach

Notification to Authorises	
Please indicate whether any authorities have been notified of the data breach. If so, please provide any reference numbers.	
☐ Police ☐ National Fraud Agency ☐ Other: Click here to insert text	☐ Bank ☐ Insurance

Information to Other Stakeholders
Please indicate whether any communications have gone out to Advance HE stakeholders (colleagues, CEG, Board etc.)

Information to Public
Please indicate whether any communications have been made public on the data breach.

Risk Assessment

To be completed by the Data Protection Officer.

Date Reviewed:	

Risk Assessment	☐ Low ☐ Medium ☐ High ☐ Critical

Data Protection Officer Comments

DPO Action Plan		
Action	**Pers Resp**	**Deadline**

ICO Reportable Breach

To be completed by the Data Protection Officer.

Is the Incident Reportable?	Yes ☐ No ☐
Date Reported:	

ICO Response:

ICO Action Plan		
Action	**Pers Resp**	**Deadline**