

Data Protection Policy

DP/01

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

1	Purpose	4
2	Scope	4
3	Definitions	4
4	Roles and Responsibilities	6
5	Commitment to Data Protection	7
6	Collecting Personal Data	7
7	Lawful Basis	8
8	Purpose Limitation	10
9	Data Minimisation, Data Accuracy & Retention	10
10	Security	11
11	Use of Innovative Technologies	12
12	Restricted International Transfers	13
13	Third Party Processors	13
13	Transmission of Personal Data	13
14	Personal Use of Personal Data	14
15	Automated Processing & Decision-Making	14
16	Cookie Management & Tracking	14
17	Direct Marketing	15
18	Information Commissioner	15
19	Record Keeping	16
20	Training and Awareness	16
21	Related Documentation	16
22	Regional Variations	17
23	Additional Information	17

Advance HE Data Protection Policy

1 Purpose

- 1.1 In order to provide its services to its stakeholders, Advance HE collects and use individual's personal data as part of its' everyday business activities.
- 1.2 Advance HE understands and is committed to ensuring the business activities that involve the use of individual's personal data are in line with the UK Data Protection Act, Data Use and Access Act and the Privacy Electronic Communications Regulations, collectively known as UK Data Protection legislation.
- 1.3 In addition to this, Advance HE will ensure that it supports any international laws and regulations when it comes to the processing of personal data from international data where appropriate.

2 Scope

- 2.1 This Policy sets out Advance HE's processes in relation to the key principles of Data Protection.
- 2.2 The Policy applies to all the personal data that is processed, regardless of the media on which that data is stored or whether it relates to customers, prospective customers, clients or support contacts, shareholders, website users or any other data subject.
- 2.3 All Advance HE colleagues must read, understand, and comply with this Policy when processing personal data on behalf Advance HE under their employment or contract with Advance HE.
- 2.4 Related policies and guidance are available to support in interpreting and acting in accordance with this Policy. Colleagues must also comply with all such related policies and guidance.
- 2.5 This Policy is an internal document and cannot be shared with third parties, clients, or regulators without prior authorisation from the Data Protection Officer.
- 2.6 The specific terms of this Policy also do not apply to disclosure of financial or other information to Advance HE accountants or for audit purposes, although Advance HE will ensure such processing is in line with the UK Data Protection legislation.

3 Definitions

Term	Definition
Automated Decision-Making	When a decision is made which is based solely on the automatic processing of personal data (including profiling) which has legal effects or significantly affects an individual. UK GDPR prohibits automated decision-making unless certain conditions are met.

Term	Definition
Automated Processing	Any operation, or set of operations, which is performed on personal data by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure, or destruction.
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.
Consent	Agreement freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.
Control of Personal Data	Advance HE has received the information on the basis that, subject to this Policy, the law and any privacy statement accepted by the data subject, that it can process their personal information as decided and without further reference to the data subject.
Data	Information which is stored electronically or in paper-based filing systems.
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 Processors	Individuals / organisations who processes personal information on behalf of a data controller. Colleagues are excluded from this definition.
Data Protection Impact Assessment	Assessment used to identify and reduce the risks of a data processing activity. DPIA can be carried out as part of the long-standing data protection principle of privacy by design and should be conducted for all major system or business change programs involving the processing of personal data.
Data Protection Officer	Individual appointed under the UK GDPR with designated responsibility for data protection compliance.
Data Subject	All living individuals about whom Advance HE holds personal data.
Data Users	All colleagues, and other individuals whom are permitted to use personal data that Advance HE controls. Data users have to follow Advance HE data protection and security policies at all times.
Information Commissioner's Office	The ICO is the UK's independent body set up to uphold information rights.
Innovative Technologies	Innovative technologies refer to new or significantly improved technologies, such as Artificial Intelligence platforms, which brings advancements in how tasks are performed.
International Transfer	Personal data originating in one country is transferred across borders when it is transmitted, sent, viewed or accessed in or to a different country.
Lawful Basis	Refers to the legal justification for processing personal data.
Personal Data	Information relating to an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier.

Term	Definition
Privacy by design	The requirement to consider and integrate data protection and privacy at the early design stage of any business practice or project which will involve personal data processing, through its lifecycle.
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.
Scientific Research	Under the Data Use and Access Act, scientific research is defined at <i>“any research that can reasonably be described as scientific, regardless of whether it is publicly or privately funded, or conducted as a commercial or non-commercial activity.”</i>
Special Category Data	Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or conditions, sexual life, sexual orientation, biometric or genetic data or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special category data can only be processed under strict conditions.
UK Data Protection Legislation	This will incorporate the following UK regulations which Advance HE s required to adhere to; UK Data Protection Act, Data Use and Access Act and Privacy Electronic Communications Regulations.

4 Roles and Responsibilities

4.1 The **Data Protection Officer** has the following responsibilities under this Policy:

- To oversee the Data Protection provision at Advance HE, ensuring there is compliance with UK Data Protection legislation.
- To be the point of contact for all internal and external data protection related queries.
- To be the direct contact with the Information Commissioner’s Office (ICO).
- Provide advice and guidance on data processing activities.
- Conduct investigation on any breach of compliance with UK GDPR, and report to the ICO if necessary.
- Ensure there is internal compliance with this Policy.
- Produce reports on the data trends for management review.

4.2 The **Audit, Finance and Risk Committee** have delegated responsibility from the Board of Directors to oversee the compliance framework with Data Protection.

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

- Ensure Advance HE has sufficient security measures as per the requirements of privacy by default and privacy by design.
- Ensure that the technical and organisational measures are effective and efficient for the processing activities carried out by Advance HE.
- Conduct regular testing on the security measures.

- 4.4 All **colleagues** have the following responsibilities under this Policy:
- Manage and maintain any data records that fall under their role in line with the UK Data Protection legislation.
 - Comply with this Policy, and all further policies and guidance under Data Protection.
 - Attend any training provided in relation to this Policy, its requirements, and any other Data Protection training offered by Advance HE.
 - Notify the Data Protection Officer of any processing activities they undertake, Data Protection queries or concerns, and breaches of Data Protection.
 - To be familiar with all Data Protection policies and procedures and ensure that they read all updates.

5 Commitment to Data Protection

- 5.1 Advance HE is committed to complying with Data Protection legislation, including assisting data subjects to exercise their legal rights in relation to their personal data which is under Advance HE's control.
- 5.2 Advance HE adheres to the principles set out in the UK Data Protection legislation which requires personal data to be:
- Processed lawfully, fairly and in a transparent manner.
 - Collected only for specified, explicit and legitimate purposes.
 - Adequate, relevant, and limited to what is necessary in relation to the purposes for which it processed.
 - Accurate, and where necessary, kept up to date.
 - Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.
 - Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful access or use, and against accidental loss, destruction, or damage.
 - Not transferred to another country without appropriate safeguards being in place, and
 - Made available to data subjects, and data subjects are allowed to exercise certain rights in relation to their personal data.
- 5.3 Advance HE commitment applies to its handling of the personal data for the duration that it is under its control. It applies to the obtaining, collection, storage, processing, and destruction of personal information, and where it may be transmitted or make it available to third parties.

6 Collecting Personal Data

- 6.1 Advance HE collects, holds, and uses significant quantities of personal data in both electronic and paper form.
- 6.2 Advance HE may collect the following personal data, but is not limited to:
- Identifiable information, such as names, date of birth etc.
 - Contact information.
 - Employment information.
 - Educational information

- Financial information
- Special category data, such as race, ethnic origin, political, religious beliefs, sex life, and sexual orientation.

6.3 Advance HE collects this personal data from customers, business and other contacts, and institutions including, but not limited to, their students, suppliers, and staff.

6.4 When collecting personal data from data subjects, Advance HE will provide Privacy Notices that outline what information will be held about them, how the data will be processed, any data transfers, and third-party use.

6.5 Advance HE may collect personal data in a variety of ways, both directly from the data subject themselves, or indirectly from a third-party source who have the authority to transfer the data, such as publicly available data or from institutions to process the data on their behalf.

6.5.1 When collecting personal data indirectly, Advance HE will ensure by all reasonable means necessary to inform the data subjects of the collection of their personal data and the purposes of processing, where it is Advance HE's responsibility to do so and will not involve a disproportionate effort to do so. Advance HE will endeavour to do this within one calendar month of collection.

7 Lawful Basis

7.1 There are a number of lawful basis for processing data which Advance HE regularly rely on for collecting, storing and processing personal data. The main lawful basis includes, but are not limited to:

Lawful Basis	Additional Conditions
Performance of, or preparation for, a contract	<p>Advance HE is procured by organisations to provide its services, these come along with a requirement to process personal data in order to meet the contractual obligations.</p> <p>In addition to this, Advance HE may procure third-party organisations to support with the delivery of services which requires sharing of personal data.</p>
Consent	<p>In some circumstances Advance HE will rely on the data subject's consent as the basis for processing their personal data, which is obtained in conjunction with their agreement to Advance HE Privacy Policy, or a relevant Privacy Notice.</p> <p>Advance HE will ensure that data subjects freely give their consent, in a specific, informed, unambiguous way on a voluntary basis.</p> <p>Advance HE will not start processing any personal data without the consent of the data subject if they are relying on the lawful basis of consent.</p> <p>Where practical and appropriate, Advance HE will give distinct options to consent separately to different purposes and types of processing.</p>

	<p>Advance HE will avoid, where possible, making consent a pre-condition of a service, except where the processing is a necessary to perform that service, i.e. surveys or applications.</p> <p>Advance HE will keep a record of consent obtained by the data subject, to ensure the consent is valid and verifiable, and to allow Advance HE to store and process the data in the ways set out for the duration of their consent.</p> <p>Advance HE will ensure that data subjects can exercise their right to revoke their consent at any time. Advance HE will endeavour to adhere to this right, where reasonably practicable and proportionate to the request.</p> <p>Under the Data Use and Access Act, Advance HE may seek consent from data subjects where specific purposes of scientific research are not fully now and is not required to provide information in the form of a Privacy Notice if it is deemed as a disproportionate burden.</p>
Legitimate interest	<p>When relying on the lawful basis of legitimate interests, Advance HE will endeavour to only use personal data in a way that the data subject may reasonably expect and to contact them without undue frequency.</p> <p>Under the Data Use and Access Act, Advance HE may apply legitimate interests to direct marketing and for the security of network and information systems.</p>
Recognised legitimate interests	<p>The Data Use and Access Act introduces the new lawful basis of “recognised legitimate interests” which may be applied in the following circumstances:</p> <ul style="list-style-type: none"> • Disclosures for the Purposes of Processing: Allowing organisations to respond to requests for information from public bodies for the purposes of public tasks. • Emergencies: Personal data which is required to respond to an emergency, under Part 02 of the Civil Contingencies Act 2004. • Crime: Organisations can use personal data for the purposes of detecting, investigation or preventing a crime, apprehending or prosecuting offenders. • Safeguarding: To protect vulnerable individuals from harm.

7.2 Regardless of which lawful basis Advance HE relies upon to collect and process personal data, Advance HE endeavours, where reasonably possible to do so, to make data subjects aware of their legal rights in relation to their personal data. Data subjects’ rights are outlined in the Data Subject Requests Policy, Privacy Policy and all Privacy Notices.

7.3 Advance HE may process or disclose personal information for lawful purposes not described in this Policy, including but not limited to for the prevention or detection of crime, or as required by regulators or by order of the Courts.

8 Purpose Limitation

- 8.1 Advance HE will ensure that all personal data it collects is only collected for specified, explicit and legitimate purposes and will not be processed in any manner incompatible with those purposes.
- 8.2 The purpose of processing will be outlined in the Advance HE Privacy Policy or relevant Privacy Notice that is shared with data subjects.
- 8.3 If Advance HE proposes to use personal data for purposes that are new, different, or incompatible with the purposes already disclosed when the data was first obtained, the data subject will be informed of the new purposes, and consent may be obtained again where necessary.
- 8.4 In certain circumstances, Advance HE may wish to reuse personal data it has collected for purposes which can be considered as compatible with the original purpose for which the personal data was collected. Compatible reasons may include:
- Responding to requests for information from a public body who confirmed they have confirmed they need the information for that purpose and to safeguard a public interest objective.
 - Archiving in the public interest.
 - Public security
 - Emergencies, and crime.
 - Protection of vital interests of data subjects.
 - Safeguarding vulnerable individuals.
 - Legal obligations.
- 8.5 Where data has been suitably anonymised, to the extent that it is not possible to identify any data subjects, it will no longer constitute personal data and Advance HE may retain and use it for any purpose. To confirm suitability for anonymisation, a data protection anonymity test will be conducted.

9 Data Minimisation, Data Accuracy & Retention

- 9.1 Advance HE will ensure that all personal data collected will be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Advance HE will ensure that all personal data collected will be accurate and kept up to date.
- 9.2 Advance HE colleagues may only process personal data when and to the extent that it is required to perform the duties of their job or contract for service(s). They may not process personal data for any unrelated reasons or collect excessive, unnecessary data.
- 9.3 Colleagues must maintain the accuracy of personal data and should not include any opinions of themselves or others within the data set.
- 9.4 Advance HE will only retain personal data for as long as necessary for the purposes the data is processed, need for legitimate business purposes, legal, accounting and reporting requirements. When personal data is no longer needed for specified purposes, it should be either retained, deleted, or anonymised in accordance with Advance HE's Retention and Erasure Policy.

- 9.5 After the retention periods, Advance HE will ensure the deletion of the personal data from all servers and filing systems. This includes requiring third-party to delete such personal data where applicable.
- 9.5.1 Hard copy versions of personal data are to be confidentially shredded, preferably at one of Advance HE's offices.
- 9.5.2 Electronic versions of personal data are to be wiped from all servers, and any storage media used must also be wiped.
- 9.6 Advance HE will conduct regularly audits of databases to ensure that any personal data is not kept longer than expected.
- 9.7 To ensure accuracy and retention is maintained, colleagues must ensure that they consider retention periods and the accuracy of their data as part of their day-to-day working operations. However, it is required that colleagues conduct regular data cleanses, at least annually.
- 9.8 Any data that cannot be confirmed as being accurate must be marked as unreliable and taken out of active circulation. Unreliable documents will be archived or destroyed in line with the Retention and Erasure Policy.

10 Security

- 10.1 Advance HE will ensure that appropriate security measures are in place against unlawful or unauthorised processing of personal data, unlawful processing, and against the accidental loss, destruction, or damage of personal data.
- 10.2 These security measures will ensure the confidentiality, integrity, and availability of personal data:
- **Confidentiality:** only authorised colleagues and approved third parties can access the data.
 - **Integrity:** personal data should be accurate and suitable for the purpose for which it is processed and protected from being damaged or corrupted.
 - **Availability:** as appropriate, Advance HE will restrict access to personal data held, and will protect it from unexpectedly being lost or unavailable.
- 10.3 Advance HE develops, implements, and maintains safeguards appropriate to its size, scope and business, available resources, amount of personal data owned or maintained and any identified risks.
- 10.4 These safeguards will be retained on a technical and organisational measures log which identifies the details of the security measures, and their application to Data Protection.
- 10.5 Advance HE will regularly evaluate and test the effectiveness of these safeguards to ensure security on the processing of personal data.
- 10.6 Advance HE IT systems, including email and internet usage, are subject to automated logging and monitoring, including the use of active monitoring.

11 Use of Innovative Technologies

- 11.1 Advance HE understands the benefits of using innovative technologies, such as Artificial Intelligence, can have on its operations. However, it also recognises the risks such technology can pose on the security of Advance HE's and data subjects' data.
- 11.2 Colleagues are not permitted to use any innovative technologies, including Artificial Intelligence platforms, without seeking prior authorisation from the IT Team and the Data Protection Officer.
- 11.3 The Data Protection Officer will conduct a Data Protection Impact Assessment on any new innovative technologies which are to be introduced to Advance HE. This is to ensure that any risks to the organisation and data subjects are identified and mitigated.
- 11.4 Advance HE recognises the following key risks when using innovative technologies and impacts these mitigating measures:

Risk	Mitigating Measures
Loss of control of data	<p>During the process of using innovative technologies, there is unclear ownership of the output data which may result in third parties having rights over the use of the data.</p> <p>Advance HE will ensure that it retains full rights and ownership over the output data.</p>
Data being used for third-party training	<p>Innovative technologies have the ability to train itself off the data that is inputted. This can mean that inappropriate disclosure to third-parties who could benefit from the use of Advance HE data.</p> <p>Advance HE will not implement any technologies which will train itself on Advance HE data. Where it does use technologies that trains itself, Advance HE will ensure that the platform remains in full control of Advance HE and no data will be used to benefit any third-parties.</p>
Inaccurate and discriminating outputs	<p>The outputs that are presented by innovative technologies, particularly those which processes personal data, may create inaccurate or discriminating outputs. This is due to the algorithms being unable to take into account non-bias factors.</p> <p>Advance HE will ensure that all outputs are checked by a human colleague.</p>

- 11.5 Where Advance HE will use innovative technologies, it will where reasonably possible, notify the data subjects of the platforms and data used. This will usually be via relevant Privacy Notices.

12 Restricted International Transfers

- 12.1 Advance HE is a global organisation who utilises various sub-processors which may require the transference of data outside of the UK and the European Economic Area (“EEA”) in order to deliver a contract or service.
- 12.2 Advance HE may undertake restricted transfers, if one of the following conditions applies:
- a) **Adequacy Decision:** the ICO has issued an adequacy decision confirming that the country to which the transfer will take place ensures an adequate level of protection for the data subjects’ rights and freedoms.
 - b) **Appropriate Safeguards:** Measures in place such as binding corporate rules, standard contractual clauses approved by the ICO, International Data Transfer Agreement, or an approved code of conduct or a certification mechanism.
 - c) **Exceptions:** the UK Data Protection legislation sets out eight exceptions that allows for international transfer without one of the above conditions.
- 12.3 If a colleague is aware that personal data will be transferred internationally, they are to notify the Data Protection Officer who will perform a Transfer Risk Assessment and put in place the relevant restricted transfer conditions.

13 Third Party Processors

- 13.1 Advance HE may appoint third party organisations / individuals (“sub-processors”), including Associates and cloud storage providers, to conduct processing on its behalf.
- 13.2 In the circumstances a sub-processor is required, the relevant Privacy Notices contain the information of the processors being used and for what purposes.
- 13.3 When appointing the sub-processors, Advance HE will follow its Procurement Policy which includes the requirements of Data Protection, including a review of the security measures in place and the completion of a Vendor Risk Assessment if required.
- 12.4 Sub-processors will have the relevant contractual agreements in place to include data sharing clauses and Data Protection measures, where appropriate.
- 12.5 All sub-processors are required to comply with Advance HE procedures and policies which are relevant to data security.

13 Transmission of Personal Data

- 13.1 When Advance HE sends out personal data, it will ensure that it is transmitted by secure means. This includes:
- Minimise the amount of personal data which is transmitted, and where possible by anonymising or pseudonymising.
 - Where personal information is to be transferred in hard copy form, it will be passed directly to the recipient.
 - When transmitting data via email, the sender must ensure they check the email for the following:
 - The recipient(s) is correct.
 - Attachment contains the correct information.
 - If there is an email chain, any personal data that should not be transmitted is removed.

- Email addresses are BCC if applicable.
- Ensure all attachments are encrypted, and passwords sent separately.
- Email address should be verified prior to sending the personal data.
- Advance HE ensures that it maintains a secure network and all emails sent are encrypted. Colleagues are not permitted to use unsecure networks to transmit personal data in any circumstances.
- Posting personal data should be avoided unless it is absolutely necessary, and no other alternative method can be used.
- All personal data sent via post should be on an encrypted USB stick and provide the password to the intended recipient by separate correspondence.
- Colleagues must avoid sharing personal data over the phone to any recipient. However, they are able to accept receipt of personal data as long as they have verified the authority of the caller as being able to share the data.
- All personal data transmitted should be clearly marked as 'private and confidential' or 'strictly confidential' where appropriate. This includes adding the relevant statement to files names, email headings and watermarks on documents.

14 Personal Use of Personal Data

- 14.1 Under no circumstance are colleagues authorised to use personal data that has been obtained via their work at Advance HE for their own personal use.
- 14.2 Colleagues are not permitted to use personal accounts, storage providers or equipment to transmit personal data on behalf of Advance HE.
- 14.3 Only under special circumstance will Advance HE permit the use of personal equipment and accounts to transmit personal data; however approval is to be sought and the IT department will be required to check security on these devices. For further information, please refer to the Acceptable Use Policy.

15 Automated Processing & Decision-Making

- 15.1 Advance HE may require the use of automated processing or automated decision-making in order to provide its services; these include cookies and personalisation / marketing activities.
- 15.2 Advance HE uses a "lead scoring" model as part of its marketing and sales process. This means when a data subject interacts with Advance HE, their data is collected and retained to determine their interests for marketing and product development purposes.
- 15.3 This information is scored and once the lead score reaches a certain threshold this may trigger an automatic process for marketing sales and communications. Data subject must give their consent for marketing communications in order to trigger this automated process.

16 Cookie Management & Tracking

- 16.1 Advance HE uses cookies and tracking on its website to support with improvements to the website, services, and products.
- 16.2 Data subjects are presented with a cookie banner and have the opportunity to consent to cookies which are not exempt from consent and may choice which cookies to consent to.

Data subjects have the right to reject the use of cookies and still utilise the Advance HE website.

- 16.3 Under the Data Use and Access Act, Advance HE will automatically opt-in devices to the following cookies:
- Cookies which are essential to transmit communications, such as for network management.
 - Cookies which are essential for services required by users, such as fraud prevention or shopping cart functionalities.
 - Collecting usage data to improve services, which are not for used for tracking or identifying users.
 - Adapting service appearance based on user preferences and accessibility requirements.
- 16.4 Data subjects will have to ability to opt-out of these cookies by making the amendments to the cookie banner.

17 Direct Marketing

- 17.1 Advance HE uses direct marketing to individuals in order to promote its products and services.
- 17.2 As Advance HE is a charity, under the Data Use and Access Act, it may market to data subjects who have previously expressed an interest in its offerings without obtaining explicit consent. This means should an individual provide their email address where and they have provided their support or expressed an interest in the charity's objectives can be directly marketed to, this is known as soft opt-in.
- 17.3 All other forms of direct marketing, Advance HE will ensure that it relies on the lawful basis of consent or recognised legitimate interest when direct marketing, this means that Advance HE will not market to any data subject unless they have given their consent to receive marketing communications, or the recognised legitimate interest of the communication balances out the data subject rights and freedoms.
- 17.4 Data subjects whether giving their consent or being soft opted-in will be able to unsubscribe from marketing communications by following the "opt-out" option at the bottom of all direct marketing communications. Following these requests, the data subject's information will be removed from Advance HE's direct marketing register.

18 Information Commissioner

- 18.1 Advance HE appoints a Data Protection Officer who is responsible for working closely with the Information Commissioner to ensure that Advance HE remains compliant with UK Data Protection legislation.
- 18.2 Advance HE is registered with the Information Commissioner and pays an annual fee to maintain this registration.
- 18.3 The Data Protection Officer is required to report any significant data breach in the UK Data Protection legislation to the Information Commissioner, if after their initial investigation determines reporting meets the threshold.

- 18.4 The Information Commissioner may conduct their own investigation following a report from the Data Protection Officer or an external individual raising a concern on compliance.
- 18.5 Should the Information Commissioner determine that a breach has occurred at the fault of Advance HE, then they may issue a fine based on the significance of the breach with remedial measures.

19 Record Keeping

- 19.1 Advance HE is required to keep full and accurate records of all its data processing activities, in line with the UK Data Protection legislation.
- 19.2 Advance HE keeps and maintains accurate records of Data Protection activities such as Records of Processing Activities, consent management, data breach register, data subject request register, vendor, and contracts management, and Data Protection Impact Assessment and risk management records.
- 19.3 Any new data processing activity must be reported to the Data Protection Officer to ensure that the correct data protection documentation is implemented, and records are up to date.
- 19.4 Advance HE also aims to regularly evaluate and review: methods of collecting, holding, and processing personal information; and the performance of employees, contractors, agents, consultants, partners or other parties working on our behalf in handling personal information, to ascertain how it can improve further.

20 Training and Awareness

- 20.1 The Data Protection Officer, in conjunction with the Learning and Development Manager, will ensure that colleagues undertake the mandatory training and any specialist training sessions covering data protection principles, policies, and procedures in place.
- 20.2 All new colleagues must undertake mandatory online data protection training within their probationary period as part of their onboarding.
- 20.3 Colleagues must undertake mandatory online data protection refresher training every two years. Failure to complete mandatory compliance learning could result in the extension of probationary period or disciplinary action against the colleague.
- 20.4 In addition to mandatory training, regular learning campaigns will be delivered to ensure colleagues are kept informed of the latest trends, changes in policies and best practice.
- 20.5 Colleagues who have a more significant role in data protection will receive the necessary training and support to meet the additional requirements within their roles.
- 20.6 Training records, including certificates, will be maintained in a log and each colleagues individual employee records of performance.

21 Related Documentation

- 21.1 The following documents should be read in conjunction with this Policy:
- Privacy Policy
 - All other Data Protection Policies, including Retention and Erasure Policy, Data Subject Rights Policy etc.
 - Data Protection Internal Guidance

- Direct Marketing Internal Guidance
- Information Technology Security Policy
- Disciplinary Policy
- Learning and Development Policy

22 Regional Variations

- 22.1 Advance HE is a registered UK company, and therefore all activities must adhere to the UK Data Protection legislation.
- 22.2 However, as it is an expanding global organisation, with bases in Ireland and Australia, Advance HE will take into consideration any additional data protection practices for that region so far as it does not interfere with UK Data Protection legislation.

23 Additional Information

- 23.1 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.
- 23.2 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.
- 23.3 Anyone found to be in breach of this Policy may be subject to disciplinary action up to and including dismissal or take legal action.
- 23.4 This Policy does not form part of any colleagues' contractual terms and conditions and Advance HE may choose to alter it at any time.