Data Protection & Confidentiality Policy

Introduction

ACME is committed to data protection as a standard and supports the data protection rights of all those with whom it works, including, but not limited to, staff, students, visitors, alumni and collaborators. This policy sets out the accountability and responsibilities of the ACME, its staff and its students to comply fully with the provisions of the UK General Data Protection Regulation ("the UK GDPR") and the Data Protection Act 2018 ("the DPA") and recognizes that handling personal data appropriately and in compliance with data protection legislation enhances trust, is the right thing to do and protects the school's relationship with all its stakeholders.

The school holds and processes personal data of individuals such as students, graduates, employees and others. Such data must only be processed in accordance with the UK GDPR and the DPA. The school has a dedicated staff who handles, monitors and provides advice on compliance with the UK GDPR and the DPA. Responsibility for compliance and the consequences of any breach, however, cannot legally be transferred to this officer but instead remains with the business space. It is expected that this policy be accompanied by a Data Strategy Handbook, which provides information and guidance on different aspects of data protection. The Handbook and the Policy outline the framework, which data processing personnel should follow to ensure compliance with data protection legislation. This policy is aligned to all information obtained from the Information Commissioner's Office (ICO) and covers the following areas:

- Purpose of the policy
- Scope of the policy and information held
- The purpose of data collection and processing
- Status of the policy
- Compliance
- Data protection by design and default
- Responsibilities under the policy
- Handling of Research data
- Data subject rights
- Student consent
- Access to information
- Data sharing (Internal and External)
- Direct marketing
- Data protection training
- Data protection breaches

2. Purpose

The purpose of this Policy is to affirm ACME's commitment to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data as per the UK Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). These ensure that data about individuals are processed with their knowledge, that data are processed with their consent in writing, verbally or by accepting to comply with the extant laws governing data protection in the UK. It also, wherever possible, offers them the freedom to have access to their personal information if necessary. This should be read in conjunction with the Information Communication & Technology (ICT) Acceptable Use Policy Guidelines and Procedures.

October 2023 Version 8.0 Next Review: October 2024 Page | 1

3. The Scope of this Policy and Information Held

This policy applies to all electronic and paper records held in filing systems containing personal data. Personal data means data that relates to an individual who can be identified by name or in any other way from the data. Like all educational establishments, ACME collects a large amount of personal data every year.

Apart from demographic information and contact details of students, staff, next of Kin and Alumni, obtained during recruitment, we also keep bank statements, educational certificates, sensitive information on ethnicity, religion, passport details, sexual inclinations, assessment outcomes and results, DBS records, student funding applications and outcomes and medical reports. Other data include any expression of opinion about an individual and intentions towards an individual, including reference letters, attestation letters and any other forms of correspondence with students. This policy also applies to data held visually in photographs or video clips, CCTV footage or as sound recordings. This policy is to be used by all staff who hold personal data on students or other employees.

4. Purpose of Data Collection and Processing

ACME, like all educational establishments, holds and processes information about its employees, applicants, students, alumni and other individuals for a variety of purposes, (for example the administration of the admissions process, the effective provision of academic and welfare services, to record academic progress, to operate the payroll and to enable seamless correspondence and communications, including the provision of references, certificates and monitoring purpose, as well as providing data to regulatory authorities for monitoring and also for research purposes.

5. Status of the Policy

In common with past data protection policies, this policy does not form part of the formal contract between ACME and staff or students, but acceptance and compliance with it forms a condition of employment and of the Student Contract to abide by the school's rules and policies. Any failure to follow the policy may therefore lead to disciplinary proceedings. Visitors and stakeholders are expected to comply with this policy in so far as they are processing data for and on behalf of the school

6. Compliance

To comply with Data Protection legislation, information collected will be obtained **with the consent** of the individual in question, stored safely, used with caution, retained for the intended period and not to be disclosed to any unauthorised persons or bodies. ACME will keep a log of all data we hold, it's sources and who we share it with. We will regard all personal information relating to students as confidential and will not divulge such information to other persons agencies or organisations without the consent of the student, except as indicated below or as required by law. Students and staff will be informed of their rights under the GDPR, including having access to all personal data held on them. Details of the six principles as set out in the Data protection legislation are found in the Data Strategy Handbook, which set out the main requirement for compliance.

Data security: All users of personal data within the school must ensure that personal data is always held securely and not disclosed to any unauthorised third party accidentally, negligently or intentionally. The Information Management Security Policy must be read in conjunction with this Data Protection Policy.

Conditions of processing/lawfulness: In order to meet the 'lawfulness' requirement, processing personal data must meet at least one the following conditions:

- The data subject has given consent.
- The processing is required due to a contract.
- It is necessary due to a legal obligation.
- It is necessary to protect someone's vital interests (i.e. life or death situation).
- It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- It is necessary for the legitimate interests of the controller or a third party.

For special categories of personal data, at least one of the following conditions must be met:

- The data subject has given explicit consent.
- The processing is necessary for the purposes of employment, social security and social protection law.
- The processing is necessary to protect someone's vital interests.
- The processing is carried out by a not-for-profit body.
- The processing is manifestly made public by the data subject
- The processing is necessary for legal claims
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services.
- The processing is necessary for public health
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards which are explained in the Data Strategy Handbook

Data retention: Personal data must not be kept longer than necessary, and for the purposes for which it was originally collected. This applies to all personal data, whether held on core systems, local PCs, laptops or mobile devices or held on paper. If the data is no longer required, it must be securely destroyed or deleted.

7. Data protection by design and default

Under the UK GDPR and the DPA, the school will always consider the impact on data privacy during all processing activities. This includes putting in place appropriate organisational measures to minimise the potential negative impact processing can have on the privacy of data subjects.

*I*mpact assessment of Data Protection: When considering new processing activities or setting up new procedures or systems that involve personal data, privacy issues must be considered at the earliest stages of planning and implementation and a Data Protection Impact Assessment (DPIA) must be conducted. The DPIA is a tool for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce privacy risks during the design stages of a process and throughout the lifecycle of the initiative.

Anonymisation and pseudonymisation: Further mechanisms of reducing risks associated with handling personal data are to apply anonymisation or pseudonymisation. Wherever possible, personal data must be anonymised or, where that is not possible, pseudonymised.

8. Responsibilities under the Policy

ACME has a legal responsibility to comply with the Act. The Senior Management Committee member with overall responsibility for this policy is the Data Protection Officer. The school is named as the Data Controller under the Act. ACME is required to notify the Information Commissioner's Office of the processing of personal data and is included in a public register of data controllers available on the Information Commissioner's website.

The Data Protection Officer is responsible for drawing a framework on good data protection practice and promoting it's compliance with this framework by advising and training staff on the creation, maintenance, storage and retention of records that contain personal information.

Every member of academic or non-academic staff that holds information about individuals has to comply with data protection in the management of that information, as individuals will be held liable for breaches of the Act.

9. Handling Research Data

Before commencing any research which will involve obtaining or using personal data and special categories of personal data, the researcher must give proper consideration to this policy and the guidance contained in the Data Strategy Handbook and how these will be properly complied with. The researcher must ensure that the fairness, transparency and lawfulness principle is complied with and that privacy by design and default is applied. This means that wherever feasible, research data must be anonymised or pseudonymised as early as possible.

The domestic use exemption applies – the school does not normally allow students to extracted data already held by the College from its database. However, in case this happens in exceptional cases, ACME remains the data controller for the database, but the student will be the data controller for the extracted data. Once a thesis containing personal data is submitted for assessment, the College becomes data controller for that personal data.

It is the duty of academic staff must ensure that students under their supervision are aware of the following:

A student should only use personal data for a College-related purpose with the knowledge and express consent of an appropriate member of academic staff (normally, for a postgraduate, this would be the supervisor, and for an undergraduate the person responsible for teaching the relevant class/course).

The use of College-related personal data by students should be limited to the minimum consistent with the achievement of academic objectives. Wherever possible data should be anonymised so that students are not able to identify the subject.

10. Data Subject Rights

The UK GDPR and the DPA contain eight data subject rights the College must comply with – the rights to information, subject access, to rectification, to object, to erasure, to portability, to restrict processing and in relation to automated decision-making and profiling. These rights can be restricted for personal data used in research.

Data subject access requests and the right to data portability: Individuals have the right to request to see or receive copies of any information the ACME holds about them, and in certain

circumstances to have that data provided in a structured, commonly used and machine readable format so it can be forwarded to another data controller. ACME must respond to these requests within four weeks. It is a personal criminal offence to delete relevant personal data after a subject access request has been received. Individuals must follow the request for access procedures outlined in paragraph 12 of this policy.

Right to erasure, to restrict processing, to rectification and to object: In certain circumstances data subjects have the right to have their data erased. This only applies where the data is no longer required for the purpose for which it was originally collected, or where the data subject withdraws consent, or where the data is being processed unlawfully. In some circumstances, data subjects may not wish to have their data erased but rather have any further processing restricted.

If personal data is inaccurate, data subjects have the right to require the ACME to rectify inaccuracies. In some circumstances, if personal data are incomplete, the data subject can also require ACME to complete the data, or to record a supplementary statement.

Data subjects have the right to object to specific types of processing such as processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right. Individuals receiving any of these requests should not act to respond but instead should contact the Data Protection Officer immediately.

1. Student Consent

Prospective Students will sign the organisation's application form and give their explicit consent to ACME holding and processing, for all relevant purposes, all data relating to them. The applicant will also consent to the school providing their information to other organisations for processing and analysis in connection with student funding, examinations and other assessments, awards, research and administration. The organisations to which ACME may provide data relating to the student as a statutory requirement include, but are not limited to, the Office for Students (OfS), Department for Education (DfE) Students Loans Company (SLC), Office of the Independent Adjudicator (OIA), Validation partners (University of Chichester) and awarding organisation (Pearson Education), Higher Educational Statistical Agency (HESA) / JISC, Quality Assurance Agency (QAA), Home Office, Local Councils and for those in receipt of benefits, the Department for Work and Pensions (DWP), In some cases, personal information is provided to such organisations through agencies acting on their behalf.

Where a student of any age is sponsored, the student will be required to confirm that the organisation can provide details of attendance, progress, achievements and other relevant matters to the sponsor.

2. Access to Information

Students and employees have rights of access to information about themselves in accordance with the provisions of the Data Protection legislation and the right to decline to be contacted by the organisation for marketing purposes.

The organisation will annually confirm the data held with each student and employee and confirm their acceptance to hold and process this data.

Students or staff who want access to their personal data are required to do so formally. A

response will be given within one month of the request at no additional cost to the student or staff. Repeated requests, however, will incur an administrative charges. This will depend on the volumes and size of data required.

If ACME refuses a request for data, the individual will be informed in writing with reasons why their request cannot be fulfilled within a maximum of one month. Further details on access to information will be found in the ACME Staff Guidelines on Dealing or Hand

3. Data sharing (Internal and External)

Internal data sharing: When personal data is transferred internally, the recipient must only process the data in a manner in accordance with the original purpose for which the data was collected. If personal data is shared internally for a new and different purpose, a new privacy notice will need to be provided to the data subjects.

External data sharing: When personal data is transferred externally, a legal basis must be determined and a data sharing agreement between the College and the third party must be signed, except the law requires disclosure. This may be the case for certain requests from organisations such as the Department for Work and Pensions or Inland Revenue, or the third party requires the data for law enforcement purposes.

Transfers of personal data outside the EEA: Personal data can only be transferred out of the UK when there are safeguards in place to ensure an adequate level of protection for the data.

4. Direct marketing

Direct marketing does not only cover the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals. For ACME, this will include notifications about events, fundraising, selling goods or services. Marketing covers all forms of communications, such as contact by post, telephone and electronic messages, whereby the Privacy and Electronic Communications Regulations 2003 (PECR) govern the use of electronic means such as emails and text messaging. ACME will always comply with relevant legislation every time it undertakes direct marketing and must cease all direct marketing activities if an individual requests as such.

5. Data protection training

Staff members receive periodic training every year to refresh their memories on the data protection policy and keep abreast of any new policy or amendments of the existing ones

6. Data Breaches and Procedures for the Security of Personal Data

The school is responsible for ensuring appropriate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The school makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Human error
- Unauthorised discosure (e.g mails sent to wrong users or incorrect recipients)
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Hacking attack

At ACME, data is stored in customised information management systems designed for the

institution with password protection. Only the Data processors and the Data Protection Officer hace access to it, and unauthorised access is very unlikely. Hard copy data is stored in locked filing cabinets and in secure and fire-proof rooms with locks. Keys to such premises are made available ONLY to authorised personnel.

Staff who have access to our data are provided with specific guidelines on how to prevent breaches of data. Our data is not in the cloud system, and it is only internally accessible. As per our procedures on the Security of personal data, below are our standards:

- All keyboards must be locked when leaving the workstation unattended.
- If sending personal data by email, ensure this is encrypted before transmission. The records should be password protected and should not identify individual students by name.
- Destroy all paper and electronic records by appropriate means such as shredding or use of confidential waste sacks and appropriate deletion of electronic files (it is pertinent to note that deleting electronic files does not equate to destroying them as they are still retrievable.
- Ensure any computer equipment that is sold or given to another institution or staff for use at home is wiped clean of all personal data.

Personal information discussed about students and staff in meeting minutes will not identify students and staff by name. This is important as these meeting minutes may be submitted to a third party for any reason.

The Organisation only operates within the UK and does not normally transfer data to other EU or non- EU countries. Staff who access information from the school on personal laptops from home ensure that their laptops are password protected and the screens are locked when not in use.

Staff who use student data for research purposes are also expected to abide by the guidelines on the Use of Personal Data for Research Purpose. This will include anonymising the data, informed consent from the data subject, use of secure and password protected electronic files and formulating a clear data management plan.

If staff with access to data identifies any reason to suspect that information stored has been compromised, (stolen computer, sent wrong data to a third party), the information must be reported to the Data Protection Officer.

Depending on the extent of the breach, the Data Protection Officer will make a report to the Information Commissioner’s Office and the individual/s involved.

A data subject may apply to the court for compensation if they have suffered damage (financial loss or physical injury, and possibly associated distress) if the school loses, destroys, discloses or allows access to personal data without the data subject's consent. The court will need to consider if the school has taken all reasonable care to prevent the loss, destruction, disclosure or access to this data.

7. Queries

To ensure ACME manages personal data effectively, and within Data Protection legislation, the Data Protection Officer (DPO) will undertake the role for the organisation. The DPO will report to the College Board of Directors any matters concerning Data Protection. This Policy

will be reviewed periodically, as agreed by the Governing Council, and changes will be agreed upon by same before implementation**.**