Data Protection Policy and Procedures

Contents

1.0 Purpose 3
2.0 Scope 3
3.0 Objectives 3
3.1 Legislative requirements 3
3.2 Legal bases for processing personal data 3
3.3 Consumer protection 4
4.0. The rights of data subjects 4
5.0 Implementation 6
5.1 Implementation of the seven principles for personal data protection 6
Principle 1: Lawfulness, fairness and transparency 6
Principle 2: Purpose limitation 8
Principle 3: Data minimisation 8
Principle 4: Accuracy 9
Principle 5: Storage limitation 9
Principle 6: Integrity and confidentiality 10
Principle 7: Accountability 11
5.2 Specific procedures for data processing 11
5.2.1 Data privacy by design and default 11
5.2.2 Procedure for conducting Data Protection Impact Assessments 12
5.2.3 Procedure for dealing with breaches of personal data 12
5.2.4 Procedure for direct marketing 13
5.2.5 Procedure for disclosing personal data 13
5.2.6 Procedure for data sharing 14
5.2.7 Procedure for the restricted transfer of private data 15
6.0 Responsibilities for data protection 16
6.1 ECT's responsibilities as the data controller 16
6.2 Responsibilities of the Data Protection Officer 16
6.3 Responsibilities of ECT staff 17
6.4 Responsibilities of service providers and short-term contracted staff 17
6.5 Responsibilities of ECT students 18
8.0 Accountabilities 18
Annexure A: Glossary 19

1.0 Purpose

The Engineering College of Technology (ECT) is committed to treating special category personal data it obtains, uses, stores and otherwise processes of its students and staff members, as well as other people it interacts and works with, in accordance with best practices and legislative prescripts. The purpose of this policy is to describe the measures ECT will implement in protecting the personal data in accordance with legal and regulatory requirements.

The policy aims to fulfil the reasonable expectations of its data subjects in relation to the processing of their personal data by ensuring that:

- ECT processes the personal data of its data subjects in compliance with legislative requirements as well as data protection principles and good practice.
- The personal data of its data subjects is protected and promoted in ECT's policies, procedures and practices.
- The staff, students and the broader ECT Higher Education community is adequately informed of the prescripts in this policy and the importance of adherence to them.
- ECT is protected from the risks of breachers of personal data that it holds of its data subjects and other breaches of data protection law.

2.0 Scope

The policy applies to the personal data of ECT's community, which includes potential, previous and current staff and students, consultants, service providers, website users and others it interacts with as a Higher Education institution, which are referred to in this policy as 'data subjects'. The broader term 'personal data' used in this policy includes 'sensitive personal data', i.e. special categories of personal data that require additional protection.

The policy applies to all personal data that ECT processes of its data subjects in the execution of its functions across all business operations, including the administration of the student admissions and enrolment process, recruitment and employment / contracting of staff, the effective provision of academic and other services, recording academic progress, operating payroll, and the communication with all data subjects.

The policy must be adhered to by all members of staff who are involved in the processing of personal data, enrolled students as well as others who are contracted by ECT in processes that involve aspects of the processing of personal data.

3.0 Objectives

3.1 Legislative requirements

The objective of this policy is to ensure that ECT as a HE institution, executives its role as 'data controller' in accordance with legislative requirements relevant data protection, in particular:

- the Data Protection Act 2018 (Data Protection Act 2018 (legislation.gov.uk)), and
- the UK version of the General Data Protection Regulation of the European Commission (UK-GDPR: The UK-GDPR | ICO).

3.2 Legal bases for processing personal data

In adherence to article 6(1) of the UK-GDPR, ECT will not process personal data unless it is able to identify an appropriate legal basis for that processing, which will include at least one of the following.

1. Consent: the individual has given clear consent for ECT to process his/her personal data for a specific purpose.
2. Contract: the processing is necessary for a contract ECT has with the individual, or because the data subject has asked the institution to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for ECT to comply with the law (not including contractual obligations).
4. Vital interests: the processing is necessary to protect the life of the data subject and/or others.
5. Public task: the processing is necessary for ECT to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
6. Legitimate interests: the processing is necessary for ECT's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

3.2.1 Mapping of lawful bases

ECT documents the lawful basis applicable to each of its processing activities within its Records of Processing Activities (RoPA). A lawful basis matrix is maintained to ensure that each processing operation is linked to an appropriate legal basis in accordance with Article 6(!) UK GDPR.

3.3 Consumer protection

In executing its functions as data controller, ECT will also ensure adherence to the following legislative requirements that relate more generally to consumer protection:

- Consumer Contracts (Information, Cancellation, and Additional Charges) Regulations (CCRs): The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 (legislation.gov.uk)
- Consumer Protection from Unfair Trading Regulations (CPRs): The Consumer Protection from Unfair Trading Regulations 2008 (legislation.gov.uk)
- Consumer Rights Act 2015: Consumer Rights Act 2015 (legislation.gov.uk)
- Equality Act 2010: https://www.gov.uk/guidance/equality-act-2010-guidance#equalities-act-2010-legislation
- Unfair Terms in Consumer Contracts Regulations: The Unfair Terms in Consumer Contracts Regulations 1999 (legislation.gov.uk)
- Higher education: consumer law advice for providers – helping you comply with your obligations (CMA33) of the Competitions and Market Authority: Higher education: consumer law advice for providers - GOV.UK (www.gov.uk).

4.0. The rights of data subjects

ECT will respect the eight rights of data subjects relating to their personal data as contained in the UK-GDPR and inform data subjects of how they can exercise these rights.

1. The right to be informed: ECT will provide data subjects with information relating to the processing of their personal data, which includes:
    - the categories of data that are obtained
    - any third-party source from which their personal data was obtained
    - the purposes for which data is obtained and processed
    - how long it will be retained and the conditions under which the periods will be extended
    - the circumstances under which it will be shared with any third parties and the safeguards that will apply

- their rights as data subjects, including their right to complain to the Information Commissioner's Office (ICO) if they believe that ECT has violated their rights in any way and/or has not taken appropriate corrective action (https://ico.org.uk/make-a-complaint).

2. The right of access: ECT will respect the rights of data subjects to request access to their personal data that is held by the institution and will provide copies of the personal data processes in response to such requests. ECT will acknowledge receipt of a Subject Access Request (SAR) without undue delay and ordinarily within 2-3 working days. ECT will respond to SARs within one month of receiving a valid request, in accordance with Article 12(3) UK GDPR. Where a request is particularly complex, or where ECT receives multiple requests from the same individual, the response period may be extended by up to a further two months. In such cases, ECT will notify the individual of the extension and explain the reasons for it within the one-month period. SARs will normally be handled free of charge. However, ECT may charge a reasonable fee or refuse to act where a request is manifestly unfounded or excessive. Any such decision will be communicated in writing. Information on how to submit a SAR and the steps ECT follows when processing requests is set out in the Subject Access Request Procedure, which supports this policy.
3. The right to rectification: ECT will respect the right of data subjects to request that personal data be corrected if information that ECT holds if they discover that personal data is inaccurate or incomplete and will update the data accordingly within a reasonable time, which will be less than one month.
4. The right to erasure (the right to be forgotten): ECT will respect the right of data subjects to request the erasure of their personal data in certain circumstances, such as where the data has been unlawfully obtained or processed, or where it no longer meets the legal ground for which it was collected, or where the consent has been withdrawn and there is no other lawful basis for processing. Further information on how to submit an erasure request and how ECT assesses and processes such requests is set out in the Data Subject Rights Procedure, which supports this policy.
5. The right to restrict processing: ECT will allow data subjects to request that it limits the way it uses personal data under certain circumstances, for example, if the individual no longer want to use ECT's product or service, or wants to limit the way the data is used subsequent to the original purpose for which the data was obtained and processed, or another valid reason for the request to restrict processing.
6. The right to data portability: ECT will respect the right of data subjects to obtain and reuse their personal data for their own purposes across different services, for example to transfer academic records to another HE institution. This right only applies to personal data that an individual has provided to data controllers by way of a contract or consent. The requested personal data will be provided in a structured, commonly used and machine-readable format.
7. The right to object: ECT will respect the right of data subjects to object to the processing of personal data that has been collected on the grounds of legitimate interests or the performance of a task in the interest / exercise of an official authority. In such cases, ECT will stop processing information unless it can provide legitimate grounds for the processing that overrides the interests, rights and freedoms of the individual. ECT could refuse this request if the data processing is required for legal purposes.
8. The rights related to automated decision-making including profiling: ECT will adhere to GDPR's provisions relating to automated decisions, such as profiling (e.g. for predicting behaviours) that are made without human involvement. ECT will respect the right of data subjects to challenge such decisions and request a review of the processes, whereupon ECT will provide clarification of how the processing met the provisions or take corrective action if the provisions were not adhered to.

In addition, ECT will respect the rights of data subjects to:

- withdraw consent previously given for the processing of data
- be notified of a personal data breach which is likely to result in high risk to their rights, security or freedom.

These rights are not absolute, and the exercise of these rights will depend on the specific circumstances and whether there are reasonable and/or legal grounds for ECT not to adhere to the rights of data subjects.

ECT could refuse an individual's right to access his/her personal records in the following circumstances:

- ECT believes that giving access would pose a serious threat to the life, health or safety of any individual or to public health or public safety
- giving access would be unlawful
- giving access would have an unreasonable impact on the privacy of other individuals.
- the information relates to existing or anticipated legal proceedings between ECT and the individual
- giving access could prejudice the taking of appropriate action in the matter
- giving access would be likely to prejudice one or more enforcement-related activities conducted by, or on behalf of, an enforcement body
- the request for access is frivolous or vexatious.

5.0 Implementation

5.1 Implementation of the seven principles for personal data protection

In executing its role as data controller, ECT will implement this policy in accordance with the following seven UK-GDPR principles that serve as the fundamental building blocks of good practice for personal data protection. (The principles | ICO)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability.

Principle 1: Lawfulness, fairness and transparency

Personal data should be "processed lawfully, fairly and in a transparent manner in relation to individuals".

ECT will only process personal data for the legitimate purposes for which it was obtained in the execution of processes relating to teaching and learning, and related administrative processes, including staffing the organisation, the Information Systems for recording and processing data, the marketing of courses, etc.

ECT will post a privacy notice on its websites where it will be available to individuals from their first point of contact with the institutions. Enrolled students and employed/contracted staff will be informed of the privacy notices during induction/orientation and training sessions. The notice will state what information ECT will collect from data subjects, how the information collected will be used and the legal basis for processing personal data, together with an undertaking not to share information for marketing purposes to any external entity. The privacy

notice will be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand what happens to their personal data.

In all cases, data subjects will be informed of the reasons for which the personal data will be used. In cases where such data will be used for other reasons than those initially communicated (or when the reasons may not be obvious), the consent of data subjects will be obtained, and they will have the right to withdraw their consent. Consent may need to be renewed if personal data will be used for a different and incompatible purpose which was not disclosed when the data subject first consented, or if the consent is historic. ECT will keep records of all consents obtained in accordance with its Records Management Policy.

If a prospective student chooses not to give ECT certain information, ECT may be unable to enrol that person in a course or supply him/her with appropriate information. Anonymity and pseudonymity are not practicable in processing personal data for enrolling students, conducting teaching and learning activities and staffing the institution.

When personal data is collected directly from data subjects, for example for the recruitment and employment of staff and for the recruitment and enrolment of students, the data subjects will be provided with ECT's name and contact details, the legitimate purpose for collecting the data and how the data will be used. In cases where personal data is collected indirectly, e.g. from a publicly available source, ECT will provide the data subject with the information required by the GDPR as soon as possible after collecting / receiving the data.

The personal data that ECT will obtain from its data subjects for executing its functions as a HE institution, with could include:

- name and surname
- physical and/or postal address
- email address
- photo
- name, surname and contact details of parent / guardian or alternative contact person
- IP address, where relevant
- online behaviour (including the use of cookies)
- profiling and analytics data.

In addition to the above-mentioned, ECT will obtain and process the following sensitive personal data from data subjects, where there is a legal basis for doing so:

- racial and/or ethnic origin
- political opinions
- religious and/or philosophical beliefs
- genetic data and/or biometric data
- aspects of the person's health and disability
- the person's sex life or sexual orientation
- trade union membership.

The legal bases for processing of sensitive personal data could include one or more of the following:

- The data subject has given explicit consent to ECT for holding and processing sensitive data.
- The processing is necessary for compliance with employment law or other legal requirement.
- The processing is necessary to protect the vital interests of the data subject and/or another person where the data subject is physically or legally incapable of giving consent.

- The processing is necessary for reasons of substantial public interest or public health, provided it is subject to professional confidentiality.
- The processing is requiring for archiving purposes, for example for research or statistical purposes, on condition that:
    - the data is subject to certain safeguards (i.e., pseudonymisation or anonymisation where possible)
    - it is not used for making decisions about particular individuals
    - could not cause substantial damage/distress to an individual.

ECT will exercise particular care in ensuring the projection of sensitive personal data, which constitute a greater intrusion into individual privacy than when processing non-sensitive personal data. Access to sensitive data will be restricted to designated managers through high-level passwords to secure this data from unauthorised access, use, disclosure or loss. As with personal data generally, it should only be kept on laptops or portable devices if the file has been encrypted and/or pseudonymised. Personal data relating to criminal convictions and offences, including the alleged commission of offences or proceedings for offences or alleged offences, will be processed in accordance with Article 10 of the UK GDPR and will be handled with safeguards equivalent to those applied to special category personal data.

Principle 2: Purpose limitation

Personal data should be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes".

ECT will only use personal data of its data subjects for the purposes relating to teaching and learning, and operational and administrative processes relating thereto as a HE provider. ECT will not use personal data for entirely new, different or incompatible purposes from those disclosed when it was first obtained without informing the data subject and obtaining consent for the new purposes.

Where such data is processed for historical research or statistical purposes (e.g. to determine student enrolment trends) safeguards such as data minimisation (e.g. pseudonymisation or anonymisation) will be applied. This will ensure that the research will not be carried out for making decisions about particular individuals that could negatively impact on persons covered in the research. Student consent will be sought to allow ECT to use any data collected for research purposes. Personal data collected for this purpose will not be disclosed to other organisations.

Principle 3: Data minimisation

Personal data should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

ECT will only collect and retain personal data that is adequate to fulfil the purposes for which it was intended to be processed and will not collect and retain personal data that are not relevant for such purposes. Personal data will only be processed for performing job duties in which the data is required and will not be processed for any reason not related to specific work duties. Personal data that is no longer needed for the purposes for which they were obtained will the deleted or anonymised in accordance with ECT's policies and procedures relevant to data processing.

Principle 4: Accuracy

Personal data should be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')".

ECT will manage data in accordance with prescripts in policies and procedures to ensure that personal data is accurate, kept up to date and recorded in the correct files. Students and staff will be required to update personal data annually or when the need arises, whereupon personal data records will be updated and incorrect or incomplete data removed. In cases where a data subject requested the correction or removal of his/her personal data, this should be done and the changes communicated to the data subject within one month.

IT and other systems used for recording personal data should be continuously monitored to identify incorrect recording of data, and the system changes must be made to address any challenges that contribute to the inaccuracy of data, in accordance with ECT's IT Policy for System Administrators and Managers.

If an individual considers his/her personal information to be incorrect, incomplete, out of date or misleading, he/she can request that the information be amended. Where a record is found to be inaccurate, a correction will be made. Where the record is found to be accurate, the details of the request for amendment will be noted on the record and the individual will be informed of the outcome of the request in writing. If the individual insists that the information is inaccurate, out of date, incomplete or misleading, ECT must take reasonable33 steps to record the individuals view in a way that will be apparent to users of the information.

Where ECT corrects personal data about an individual that the entity previously disclosed to another data controller or entity, ECT must give notification to the entity of the correction of the information.

Principle 5: Storage limitation

Personal data should be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals".

ECT will inform data subjects of the periods for which their personal data is stored for the following categories of data:

- Student records will be kept electronically for a minimum of 6 years. Paper records will be limited and converted where possible. If paper records are required, then they will be stored in a lockable, fireproof, non-portable safe.
- Completed student assessment items will be kept electronically for each student for a period of six months from the date on which the assessment judgement for the student was made.

The records of personal data that ECT needs to keep for longer, e.g. for statistical or research purposes, will be safeguarded to protect the persons' privacy and confidentiality through data minimisation (e.g. pseudonymisation or anonymisation).

ECT will take all reasonable steps to destroy or erase from its record systems all personal data that are no longer required in accordance with all relevant ECT records retention schedules and relevant policies and procedures, including the Records Management Policy and IT Policy for System Administrators and Managers. Electronic record-keeping systems will be programmed to issue alerts for the removal of data at set periods.

ECT will keep full and accurate records of all our data processing activities, including records of consents given by data subjects.

Principle 6: Integrity and confidentiality

Personal data should be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

The systems and processes for ensuring the security of personal data that is processed electronically will be managed in accordance with ECT's IT Policy for System Administrators and Managers. The policy describes the roles of managers and the system administrators in managing, maintaining and monitoring ECT's ICT systems, facilities and resources. They will comply with all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction.

ECT will securely store all records containing personal data and take all reasonable security measures to protect such data from loss, interference, unauthorised access, misuse, modification or disclosure. This is ensured via storage of records in hard copy form in lockable cabinets as well as by rigorously restricting access to electronic records to selected authorised staff members . ECT will establish, maintain and continuously upgrade a set of robust and best-practice security mechanisms to protect its information technology infrastructure and electronic records.

All new software and systems must be approved and procured through IT Services, where it will be checked for technical, security and data protection compliance.

Processes for ensuring the security, integrity and confidentiality of personal data will be performed in accordance with ECT's IT Policy and associated procedures. ECT will implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage. These measures will include:

- restricting access to personal data to individuals who require it for their role and are authorised to use it
- applying elevated access controls only where necessary and ensuring users protect the confidentiality, integrity and availability of personal data
- using appropriate encryption, authentication and password-protected mechanisms
- maintaining secure systems and networks, including timely patching and system updates
- maintain processes for the secure deletion of anonymisation of personal data when it is no longer required
- implementing measures to reduce the risks of cyber-attacks, including phishing, ransomware, credential compromise and supplier-related cyber risks
- monitoring systems for unauthorised access attempts or abnormal activity, and responding promptly to potential security incidents

Further operational detail is contained within ECT's IT Policy and related technical procedures, which support this policy.

Principle 7: Accountability

"The controller must "take responsibility for what you do with personal data and how you comply with the other principles … and must have appropriate measures and records in place to be able to demonstrate your compliance".

As the data controller, ECT's Governing Board, supported by the Dean and Head of College, is accountable for adherence to the seven principles of the UK-GDPR. Therefore, the management will put in place appropriate organisational technical measures to ensure that the principles are adhered to and promoted in the collecting, processing and record keeping of personal data.

- The ECT will establish, annually review and update policies and procedures, particularly the Data Protection Policy, Consumer Protection Policy and Records Management Policy, and other policies that cover all the processes in which personal data is used in the teaching and learning and other activities of ECT as a HE training institution.
- The ECT will employ a qualified staff management team and staff and establishing structures responsible for driving the implementation of the policies and procedures, monitoring and evaluating their effectiveness, and taking corrective action where required to ensure that processes and procedures reflect data protection requirements.
- The ECT will designating a senior manager as the Data Protection Officer responsible for establishing a framework for managing personal data and promoting a culture of data protection in the organisation.
- The Data Protection Officer will conduct Data Protection Risk Assessments for processing activities that are likely to result in a risk to the interests and rights of data subjects and recommend improvements on the basis of the findings.
- Creating a culture that values and prioritises privacy issues; a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.
- ECT will provide training to all staff in data protection to promote understanding of their responsibilities in their particular work in dealing with personal data and will keep record of all such training.
- ECT will including the requirements relating to the appropriate arrangements for data protection in the written contracts with service providers that process personal data on its behalf or as part of services it provides to the organisation.
- ECT will keep record of all incidents of personal data breaches, including the facts surrounding the breach, its effects and the remedial action taken. ECT will report breaches to the Information Commissioner's Office when warranted by the likelihood and severity of the risk to people's rights and freedoms.
- ECT will improve data governance through systems that maintain accurate and up-to-date records of the processing activities of personal data and make the records available to ICO, if requested.

5.2 Specific procedures for data processing

5.2.1 Data privacy by design and default

As data controller, ECT will follow the GDPR's 'data protection by design and by default' approach to put in place appropriate technical and organisational measures to implement the data protection principles effectively to safeguard individual rights. Accordingly, data protection will be integrated into ECT's processing activities and business practices from the design stage and through the lifecycle. (Data protection by design and default | ICO)

This approach will apply to the type and volume of personal data collected, the extent of the processing, the period of storage, the accessibility of and the restriction on access to personal data, as well as measures to prevent breaches and effectively dealing with such breaches.

5.2.2 Procedure for conducting Data Protection Impact Assessments

ECT will conduct Data Protection Impact Assessments (DPIAs) to fulfill its accountability obligation under the UK-GDPR. DPIAs will be conducted before undertaking high-risk processing in order to minimise risk and determine whether the risk is acceptable in the circumstances. The DPIA will be designed to systematically analyse, identify and minimise the data protection risks of a project or plan.

Potential and real risk

Circumstances in which a DPIA will be conducted include:

- the introduction of new technologies or changing technologies such as programmes, systems or processes
- automated processing, including profiling that will lead to decisions that could have a legal effect on the individual
- large-scale processing of sensitive personal data
- large-scale, systematic monitoring of a publicly accessible area
- the introducing of a new data-sharing process with an external entity
- when any member of staff identifies the need for such an assessment.

The DPIA should include:

- the appropriate consideration of privacy by design and default
- a description of the processing, its purposes and the data controller's legitimate interests
- an assessment of the necessity and proportionality of the processing in relation to its purpose
- an assessment of the real or potential risk to individuals
- the risk-mitigation measures in place
- check compliance with data protection legislation
- adherence to the data protection principles
- the level of security needed for the personal data being processed
- the proper management of the data when it is no longer needed, either through anonymisation or destruction.

Any risks identified through the assessment will be considered and appropriate actions taken to mitigate the risk. Where warranted, the DPIA will be revisited at key stages in the project and/or when changes to the project take place.

Where a DPIA identifies a high risk to individuals that cannot be sufficiently mitigated, ECT will not proceed with the processing until it has consulted the Information Commissioner's Office (ICO), in accordance with Article 36 of the UK GDPR. ECT will follow any advice issued by the ICO as part of the consultation process.

5.2.3 Procedure for dealing with breaches of personal data

ECT has put procedures in place; procedures to deal with any suspected personal data breach that include:

- informing the designated Data Protection Officer, or relevant manager, as soon there is evidence of a real, potential breach

- notifying notify data subjects of personal data breach results in a high risk to the data subject, unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, or security measures were applied to render the personal data unintelligible (e.g. encryption)
- in cases where it is impractical to inform data subjects directly, issuing a public communication or effective alternative measure to inform data subjects, so that they themselves can take any remedial action, if required
- notifying the ICO within 72 hours where legally required to do so in cases where there is a risk to the rights and freedoms of the data subject as a result of the personal data breach
- retaining all evidence relating to personal data breaches.

5.2.4 Procedure for direct marketing

ECT may process personal data for direct marketing purposes in accordance with the UK GDPR and Privacy and Electronic Communications Regulations (PECR).

ECT will normally rely on legitimate interests as the lawful basis for direct marketing, where appropriate relationship exists and a balancing assessment has been undertaken. Where required by law, ECT will rely on consent.

Marketing communications sent by email and/or other electronic means will only be issued where permitted under PECR, including reliance on soft opt-in where applicable.

Data subjects have an absolute right to object to direct marketing at any time and marketing communications will include a clear opt-out mechanism.

5.2.5 Procedure for disclosing personal data

Communication on disclosure of personal data

ECT will publish the circumstances and conditions under which it will disclose personal information of data subjects during training sessions to staff and enrolled students and through publishing the policy on:

- ECT's website
- ECT's application form and acceptance of offer form
- ECT's Online Letter of Offer to potential students
- Online Learning Handbook for ECT students
- Documentation during ECT's staff induction
- ECT's Staff Handbook.

ECT will communicate the policy in another format to an individual upon request.

Conditions for the disclosure of personal data

ECT will only disclose an individual's personal data to another person or organisation under the following conditions:

- The data subject has given written consent to the disclosure.
- The disclosure is required or authorised under a UK Act or regulation.
- The disclosure is reasonably necessary for the enforcement of the criminal law or other legal purpose.
- There are reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life and health of the data subject or of another person.

- The individual is reasonably likely to have been aware, or made aware, that information of that kind is usually disclosed to that person or organisation.

The person/s or organisations to whom personal data is disclosed may not use or disclose the data for a purpose other than the purpose for which the information was provided.

Circumstances under which personal data will be disclosed

a) Education-related purposes

ECT may disclose the personal data of a student or potential student to persons or organisations that deliver courses in conjunction with ECT or provide education-related services to ECT in which they need access to the data for performing the services in the contract or agreement.

Personal information about students studying at ECT and course enrolment may be shared with the UK Government and designated authorities, including the Office of the Independent Adjudicator for students in higher education (OIA), Competition & Markets Authority (CMA) or Office for Students (OfS). This information could include student and course enrolment details.

b) Law enforcement or legal purposes

ECT will disclose personal data to organisations in circumstances where they have a legal right to the data or for one or more enforcement-related activities conducted by, or on behalf of, an enforcement body. This could include police or other law enforcement agencies, professional bodies, such as the Health and Care Professions Council or government agencies such as the Child Support Agency.

Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or other legal requirement, ECT will:

- seek confirmation that the organisation has the power to demand access before disclosing personal data in response to a request
- require a warrant or court order where appropriate; however, ECT may make a lawful voluntary disclosure to the police or other relevant authorities under the Data Protection Act 2018 where the disclosure is necessary for the prevention or detection of crime, the apprehension or prosecution of offenders, or the protection of individuals from serious harm
- record the disclosure in the relevant system or record, including details of what was disclosed, when and to whom

c) Personal interest

Personal data may be disclosed to parents or legal guardians who have a person interest in the person. In such cases, ECT will only share personal data with the written consent of the individual concerned, or if ECT believes that the disclosure is reasonably necessary. In the case of students under the age of 18, their consent is not required for disclosure of personal data to parents or legal guardians.

5.2.6 Procedure for data sharing

ECT will adhere to the ICO Data Sharing Code developed under section 121 of the Data Protection Act 2018 to share data fairly and lawfully in meeting its accountability obligations as data controller. (https://ico.org.uk)

The following factors will be taken into account in decisions on data sharing:

- the overall objective of sharing the data
- the potential benefits and risks to individuals and/or society of sharing or not sharing

- the fairness of sharing data in a particular way
- whether the sharing necessary and proportionate to the issue
- the minimum data that can be shared to achieve the objective
- whether the objective could be achieved without sharing personal data, or by sharing fewer personal data
- the safeguards put in place to minimise the risks or potential adverse effects of the sharing
- whether the sharing is in line with the principles for personal data protection.

Internal data sharing

Internal sharing of personal data of data subjects between staff and business units must adhere to the prescripts in this policy, including restricting access to persons / units who required access for the performance of work-related functions.

External data sharing

The sharing of personal data to external entities, such as other HE institutions should only be done:

- where there is a valid and lawful reason for the external entities to have access to the data
- with the written consent of the data subjects
- in compliance with the data protection principles
- and there must be a clear and lawful reason for doing so. Data sharing can take place in a routine, scheduled way or on a one-off basis. When needed it can be shared in urgent or emergency situations.

Data sharing agreements could be routine, scheduled or on a once-off basis. All such agreements must be in writing, stipulate the conditions of access and other manager. These agreements must be reviewed at least annually or at the end of the agreement period.

ECT will not agree to any data sharing agreements with external entities for the use in direct marketing or other marketing purposes.

5.2.7 Procedure for the restricted transfer of private data

This procedure applies to the restricted transfer of data, where:

- the UK-GDPR applies to the personal data that is being transferred
- the data is being transferred to or made accessible to a receiver (to whom the UK-GDPR does not apply) or is located in a country outside the UK
- the receiver is a separate company or individual, including another company in the same corporate group.

ECT will transfer personal data outside the UK if the country to which the data is transferred is designated by the UK as offering adequate data protection. Where there is a valid reason for ECT to transfer personal data to countries that do not enjoy this designation, ECT will undertake a risk assessment, to determine if the country ensures an adequate level of protection for the data subjects' rights and freedoms that is essentially equivalent to the protection under the UK-GDPR. If the assessment indicates that the required level of protection is not provided, ECT will implement additional protection measures to ensure that both ECT and the receiver of the restricted transfer are legally required to protect individuals' rights and freedoms in respect of their personal data. These measures may include the use of the UK International Data Transfer Agreement (IDTA) approved by the ICO or the UK Addendum to the EU Standard Contractual Clauses (SCCs).

In addition, ECT will only transfer personal data outside the UK if one of the following conditions applies:

- the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks
- the transfer falls within one of the derogations set out in Article 49 of the UK GDPR
- the transfer is necessary for the performance of a contract between ECT and the data subject (e.g. students' study at an institution outside the UK)
- the transfer is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent.

In transferring personal data outside the UK, ECT will ensure that:

- compliance checks are performed on all additional software and systems to ensure that transfer out of the UK is only done if the adequacy arrangements or necessary additional safeguards are in place
- where adequate safeguards are not in place, the personal data will be pseudonymised or anonymised so that the identify of individuals is protected.

6.0 Responsibilities for data protection

All ECT's employees and enrolled students are required to comply with this policy. Any deliberate breach of the data protection policy may lead to disciplinary action.

6.1 ECT's responsibilities as the data controller

The main responsibilities of the ECT Governing Board, supported by the Dean and Quality and Compliance Manager, will bet the following to demonstrate the institution's compliance with the law.

- Establish a governance structure with roles and responsibilities for dealing with matters relating to the protection of personal data, including designating a member of staff as a Data Protection Officer (DPO).
- Follow the UK GDPR 'data protection by design and by default' approach to put in place appropriate technical and organisational measures to secure personal data and implementing these measures in an effective manner to ensure compliance with the data protection principles.
- Document data protection policies and procedures and take measures to ensure compliance.
- Keep a detailed record of all data processing operations.
- Carry out Data Protection Impact Assessments (DPIAs) for high-risk processing operations.
- Train all staff on compliance with Data Protection Law and keep a record of such training conducted.
- Include a briefing on ECT's Data Protection Policy and students rights as part of the induction of enrolled students.
- Retain responsibility for the control of the personal data that it collects even if that data is later passed onto another organisation or is stored on systems or devices owned by other organisations or individuals (including devices personally owned by members of staff).

6.2 Responsibilities of the Data Protection Officer

The DPO is responsible for:

- Advise ECT and its staff on their obligations under the GDPR.
- Monitor ECT's compliance with the GDPR and other relevant data protection law.
- Conduct DPIAs in respect of the processing of activities that are likely to result in a risk to the interests and rights of data subjects and recommend improvements on the basis of the findings.
- Cooperate with and act as ECT's contact point for the Information Commissioner's Office (ICO).

The DPO shall act independently; shall not be instructed regarding the exercise of their tasks; and in accordance with UK-GDPR Articles 37-39.

6.3 Responsibilities of ECT staff

All the academic, administrative, support and technical staff of ECT whose work involves the processing of personal data must comply with the requirements of this policy. Their responsibilities include:

- completing ECT's compulsory annual training for staff in data protection
- ensuring that any personal data they hold is kept securely and processed in accordance with the prescripts in this policy
- ensuring that personal data is not disclosed orally or in writing or otherwise to any unauthorised third party, and taking every reasonable effort to avoid the accidental disclosure of data
- reporting any real or potential breaches of personal data to the DPO or other manager as soon as they become aware of it
- directing all third-party requests for access to personal data to the DPO
- as employees, ensuring that the personal data they supply to ECT is accurate and up-to-date
- as data subjects, monitor ECT's compliance in the way the institution obtains and processes the personal data of staff.

6.4 Responsibilities of service providers and short-term contracted staff

Service providers and short-term contracted staff who process personal data on behalf of ECT must comply with the requirements of this policy and with their contractual obligations. In accordance with Article 28 of the UK GDPR, they are required to:

- process personal data only on documented instructions from ECT
- ensure that all persons authorised to process personal data are subject to appropriate confidentiality obligations
- implement appropriate technical and organisational measure to protect the security, integrity and confidentiality of the personal data they process
- assist ECT, insofar as reasonably possible, in fulfilling its obligations in relation to data subject rights, data protection impact assessments and the management of personal data breaches
- not engage any sub-processors without ECT's prior written authorisation and ensure that any authorised sub-processor is bound by the same data protection obligations
- return or securely destroy all personal data at the end of the contract or service provision, unless retention is required by law
- make available to ECT all information necessary to demonstrate compliance with their data protection obligations and allow for audits or inspections where appropriate

In addition, service providers and contract staff must:

- refrain from accessing personal data that is not required for the performance of their contracted duties
- not transfer, store or process personal data outside the UK without ECT's prior written consent

6.5 Responsibilities of ECT students

Students are responsible for:

- familiarising themselves with the Privacy Notice provided when they enrol for ECT courses
- participating in the briefing on ECT's policies during induction sessions for enrolled students
- ensuring that their personal data provided to ECT is accurate and up to date
- adhering to the prescripts in this policy that relate to students as data subjects, including the right to lodge complaints with the Information Commissioner's Office (ICO) if they believe that ECT has violated their rights in any way and/or has not taken appropriate corrective action.

8.0 Accountabilities

The Board of Governors is responsible for annual review and approval of this policy. The Board must keep records of previous versions of the document for future reference.

The policy is to be implemented via induction and training of staff and distribution to students and ECT's community via the website and other publications.

Annexure A: Glossary

References: https://ico.org.uk/privacy notice https://ico.org.uk; *https://www.gov.uk/data-protection*; https://www.jisc.ac.uk/

Anonymisation	Anonymisation is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified. "Anonymisation means that individuals are not identifiable and cannot be re-identified by any means reasonably likely to be used (i.e., the risk of re-identification is sufficiently remote). Anonymous information is not personal data and data protection law does not apply." (https://ico.org.uk)
Automated Decision-Making (ADM)	This refers decision that are made based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The UK-GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not automated processing.
Breach of personal data	*Refer to Personal data breach*
Consent	Consent refers to an agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to him/her.
Adequacy decision	'Adequacy decision' is a term that the UK-GDPR uses to describe other countries, territories, sectors or international organisations that it deems to provide an 'essentially equivalent' level of data protection to that which exists within the UK. An adequacy decision is a formal decision made by the UK government which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for personal data as the UK does. (Adequacy decision | ICO)
Data controller	A data controller is the person, entity or organisation that determines when, why and how to collect and process personal data. It is responsible for establishing practices and policies in accordance with the UK-GDPR.
Data protection	Data protection is the fair and proper use of information about people. It is part of the fundamental right to privacy and concerns the fair and proper use of such information.
Data Protection Act	The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). The Act controls how personal information is used by organisations, businesses and the government.
Data protection law	UK data protection law is set out in the Data Protection Act 2018, along with the UK General Data Protection Regulation (UK-GDPR) which also forms part of UK law. Data protection law regulates how organisations, such as HE institutions, collect and use information about students, staff and others. It also provides individuals with the right to access information that is held about them. This legislation requires accountability and transparency from all those who collect and process any information relating to an identifiable individual (i.e. personal data).
Data subject	The identified or identifiable living individual to whom personal data relates and about whom personal data is obtained and processed.
Data Protection Impact Assessment (DPIA)	"A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK-GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations. It does not have to eradicate all risk but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve." (https://ico.org.uk)

Data Protection Officer (DPO)	This is the person appointed as such under the UK-GDPR and in accordance with its requirements. A DPO is responsible for advising the HE institution (including its employees) on their obligations under Data Protection Law, for monitoring compliance with data protection law, as well as with the institution's polices, providing advice, cooperating with the Information Commissioner's Office (ICO) and acting as a point of contact with the ICO.
UK General Data Protection Regulation (UK-GDPR)	"The UK General Data Protection Regulation (UK-GDPR) is a law that governs how organisations process personal data relating to individuals in the UK and is enforced by the Information Commissioner's Office (ICO). The UK-GDPR gives data subjects more control over how their personal data is processed and places a range of obligations on organisations that process and control the processing of their personal data. The UK-GDPR applies both to UK organisations that collect, store or otherwise process the personal data of individuals residing in the UK, and to non-UK organisations that offer goods or services to, or monitor the behaviour of, UK residents." (https://ico.org.uk)
Information Commissioner's Office (ICO)	The Information Commissioner's Office (ICO) regulates data protection in the UK and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Personal data	Personal data is "any information relating to a person (a 'data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person." (https://ico.org.uk)
Personal data breach	Personal data breach is any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can result from an act or omission.
Privacy by Design and Default	This refers to the UK-GDPR requirement that controllers put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. In essence, this means controllers have to integrate or 'bake in' data protection into your processing activities and business practices, from the design stage right through the lifecycle. Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the UK-GDPR's fundamental principles and requirements, and forms part of the focus on accountability. (https://ico.org.uk)
Privacy Notices	In the context of the GDPR, a privacy notice is a publicly accessible document produced for data subjects. A privacy notice should also explain the purposes for which personal data are collected and used, how the data are used and disclosed, how long it is kept, and the controller's legal basis for processing. It should identify who the data controller is, with contact details for its Data Protection Officer.
Processing data	Processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure. ((Data protection principles, definitions, and key terms | ICO Processing also includes transmitting or transferring personal data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.
Profiling	Profiling refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

Pseudonymisation	Pseudonymisation refers to replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure. The UK-GDPR defines pseudonymisation as "…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." (https://ico.org.uk)
Restricted transfer of data	Data transfers are restricted if: - the UK-GDPR applies to the personal data that is being transferred - the data is being transferred to or made accessible to a receiver (to whom the UK-GDPR does not apply) or is located in a country outside the UK - the receiver is a separate company or individual (including another company in the same corporate group)
Special Category Data	Special category data is personal data that is particularly sensitive and therefore needs extra legal protection under UK-GDPR. It is data that, if misused or disclosed could cause serious harm, discrimination or distress to an individual. Because of this, the law sets a higher bar before organisations are allowed to process it. This includes information pertaining to: - health data (physical or mental) - racial or ethnic origin - political opinions - religious or philosophical beliefs - trade union membership - genetic data - biometric data (where used for identification) - sex life or sexual orientation.
Transfer of personal data	The transfer of personal data originating in one country across borders when the data is transmitted or sent to a different country or for viewing / accessing it in a different country.

Document Control	
Document title	Data Protection Policy and Procedures
Version no.	2
Date Approved	March 2026
Approving Body	Board of Governors
Policy Custodian	Head of College Operations
Policy Contact	Quality Assurance and Compliance Manager
Commencement Date	March 2026
Review Period	Annually
Next Review Date	March 2027

Revision History		
Version	**Date**	**Description of key changes**
1.1	Dec 2023	Align the document to the quality assurance practices in UK universities
1.2	Apr 2024	Text on the annual review of the policy is added based on the recommendations from the Academic Board review
2	March 2026	Updates made in conjunction with the Data Protection Officer