UEL DATA PROTECTION POLICY

Version control							
Version No.	**Date**	**Equality analyses completed**	**Responsible Officer**	**Last review**	**Next review**	**Approved by**	**Date of approval**
3	**28 July 2025**	**Yes**	**Data Protection Officer**	**July 2020**	**July 2027**	**UEL Executive Board (UEB)**	**14 August 2025**

Summary

This policy explains how UEL meets its obligations under the UK GDPR and Data Protection Act 2018 and outlines our responsibilities and requirements when personal data is processed for any reason.

Definitions

'Personal data' refers to any information that relates to a living person who is, or could be identified, directly or indirectly (i.e. in combination with other data) based on the information held. Information that counts as personal data includes (but is not limited to) an individual's name, home address, email address, identification card number, location data (e.g. the location data function on a mobile phone), job title (if the individual is the only one with that title in the organisation) and image.

Some types of personal data are particularly sensitive. This is referred to as special category data, which must be treated particularly carefully. Special category data includes information such as data about race, ethnicity, religion, medical / health data, political affiliations, genetic or biometric information. Further information on special category data can be found in UEL's Privacy Statement.

A glossary of commonly used terms and definitions is provided in Appendix B of this policy and on the intranet pages.

Compliance

Complying with this policy is a condition of employment or study at UEL. Failure to comply may result in disciplinary action.

Misusing personal data or negligent disregard for the Data Protection Act 2018, or any law designed to protect personal data, could lead to prosecution and a criminal record.

This policy forms part of UEL's Information Governance Framework. It ensures ongoing compliance with Data Protection and related laws. It also promotes information governance best practices across the institution.

UEL must provide information about the processing of their personal data ensure that individuals are aware of, and can exercise their individual rights.

All staff, students and third parties associated with UEL have a responsibility to keep personal data secure. They should only use personal data for the purpose it was collected and only share it when authorised. Any students that process the personal data of others as part of their course are subject to the same conditions and to the relevant points in this policy.

Personal data processed specifically for UEL purposes on personal devices is still subject to data protection legislation. If you have a non-UEL managed device and process personal data (for example in an instant messaging application) you must comply with the UK GDPR principles.

In the event of a known or suspected data breach, staff and students have a responsibility to notify the Data Protection Officer via dpo@uel.ac.uk immediately.

The Information Assurance Office provides a range of resources and guidance to help Schools and Services comply with information law on its dedicated Intranet pages.

Scope

This policy applies to any individual or organisation that processes personal data for, or on behalf of, UEL or other businesses affiliated with our activities.

Processing of personal data refers to any action carried out to complete a task. These include, but are not limited: identifying, collecting, recording, organising, structuring, storing, altering, retrieving, disclosing (by any means), restricting, erasing or destroying personal data.

This policy applies to all processing of personal data in electronic form including electronic mail, documents created with word processing software, applications, software or, where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy sets a minimum standard for the processing and protection of personal and special category data by all UEL entities. If there are any conflicts between this policy and national law, the law will take precedence. In this case, please consult with UEL's Data Protection Officer and legal team for guidance.

Purpose of Data Collection and Processing

UEL must collect and store a wide range of personal and special category data about its employees, students and other users of UEL facilities to allow it to maintain its core operations. To comply with the law, UEL and anybody responsible for processing personal data on its behalf must:

- Have at least one valid lawful basis for processing
- Be accountable and transparent about how and why we use personal data
- Implement the appropriate controls, technical and organisational measures required to demonstrate compliance with the data protection principles
- Allow a person to exercise their Information Rights and adhere to approved codes of conduct for data protection
- Only use personal data for clear and specified purposes
- Only keep personal data for as long as is reasonably required
- Ensure that personal data is kept securely and protected against unlawful processing, accidental or deliberate loss, inaccessibility, destruction or damage

Data Protection Principles

The following principles govern the collection, use, retention, transfer, disclosure and destruction of personal data. These principles must be followed when processing personal data. Further advice and guidance for staff about how to apply these principles can be found on the Information Assurance Office Intranet site:

- Lawfulness, Fairness and Transparency - Personal data shall be processed lawfully, fairly (e.g. data subjects must not be misled) and in a transparent manner (i.e. information given to data subjects must be accessible, digestible and unhidden
- Purpose Limitation - Personal data shall be collected for specified, explicit and legitimate purposes and not used for other purposes where such use would be incompatible with the initial purpose
- Data Minimisation - Personal data shall be adequate (i.e. not too much or too little), relevant and limited to what is necessary for the purpose it was collected
- Accuracy - Personal Data shall be accurate and, where necessary kept up to date.
- Storage Limitation - Personal data shall be kept in a form, which permits identification of Data Subjects for no longer than is necessary
- Integrity & Confidentiality - Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing, and against accidental loss, inaccessibility, destruction or damage to that data
- Accountability – Where UEL acts as the Data Controller, we must be able to demonstrate how we comply with the law by ensuring that we have documented processes, procedures and policies in place

Responsibilities

The Board of Governors has delegated the responsibility for the protection of personal data at Senior Management level to a dedicated Data Protection Officer (DPO). The DPO

is authorised to act independently and has overall responsibility for ensuring ongoing compliance with UEL's data protection obligations. In order to comply with obligations, set out in the General Data Protection Regulation, the role of the DPO is autonomous and they report to the highest level of management within the organisation. The DPO's broad responsibilities can be summarised as:

- Inform and advise all parties working for, with or on behalf of UEL of their obligations and responsibilities when processing personal data;
- Monitor compliance with UK GDPR and with UEL data protection policies;
- Raise awareness and train staff involved in processing of personal data;
- Provide advice, where requested as regards Data Protection Impact Assessments and Data Sharing Agreements, and monitor their performance in terms of processing compliance;
- Act as the contact point for, and co-operate with the Supervisory Authority (Information Commission);
- Be accessible and available as the contact point for all staff, students and other appropriate third parties.

Each Dean of School or Director of Service is responsible for promoting and modelling best practices regarding data protection within their teams, and keeping the DPO informed of changes in the collection, use, and security measures used for the processing of personal data within their School, Service or unit. To meet this requirement, the Information Assurance Office will train University staff to act as Data Protection Advisors. They will promote best practices and report issues within their own departments. Senior Management, staff and students all share responsibilities for data protection, as detailed in Appendix D.

UEL staff must carry out a Data Protection Impact Assessment (DPIA) for any processing of personal data that is likely to result in a high risk to individuals (see DPO responsibilities above for more information). This is mainly for any new / additional processing activities and includes:

- Evaluation or scoring
- Automated decision-making of special category data with significant effects
- Processing of sensitive (but not special category) data or similar data of a highly personal nature
- Systematic monitoring
- Processing on a large scale
- Processing of data concerning vulnerable data subjects
- Innovative technological or organisational solutions
- Processing that involves preventing data subjects from exercising a right or using a service or contract

Business Owners are responsible for ensuring that any risks identified in a DPIA are mitigated to a level that falls within UEL's corporate risk appetite.

Information Rights

Every person about whom UEL processes personal data has rights associated with how the data is used and managed. Where an individual makes a request related to any of their information rights, UEL will consider each request in accordance with all applicable laws and regulations. Every user that processes personal data for UEL purposes is required to co-operate with the Information Assurance Office to ensure UEL complies with the legal obligations for responding to information rights requests.

Further details relating to information rights can be found in Appendix E.

Fair Processing Notices

Where UEL acts as a Data Controller, we will provide information about why and how we will process personal data. . We will also identify the circumstances under which transfers take place and provide information about routine disclosures to other parties and recipients. A complete list of UEL's Fair Processing Notices is available our website at uel.ac.uk via the Data Protection section.

Third party processing

Where UEL acts as a Data Controller, any UEL department wanting to share personal data with the other party must consult the Information Assurance Office to ensure the sharing is lawful and secure and that relevant contractual clauses outlining our requirements are agreed before processing commences.

New processing activities that involve higher-risk activities and/or special category data should be risk-assessed. See section on Data Protection Impact Assessments, above.

Where the third party is deemed to be a joint or independent Data Controller, UEL's DPO will consult with relevant colleagues to ensure our responsibilities are identified and agreed within the contract.

Information Security

All staff and students are responsible for ensuring that all personal data processed is done so lawfully and securely. This includes working onsite (e.g. on campus) and remotely. Information security and data protection are not separate or distinct from each other. The term information security is commonly used for technology (e.g. securing our systems from phishing attempts and cyber-attacks) but for the purposes of data protection and privacy, information security considerations can include:

- Keeping any personal data held in whatever format is kept secure

- Not disclosing personal data orally, in writing or electronically, either accidentally or otherwise to any unauthorised third party
- Not leaving any personal data that is taken off site unattended or unsecured
- Keeping desks clear of personal data when unattended
- Keeping personal data that exists in a manual form in a locked filing cabinet, drawer or in a secured area

For a full definition of data processing, please refer to Appendix B.

UEL staff can also refer to UEL's Information Security Policy (see Appendix A).

Remote Working

While working remotely, i.e. away from UEL places of work (i.e. office, campus, etc.), the principles and obligations of the Data Protection Act 2018 still apply. Personal data processed in remote locations, on UEL or personal devices (the latter where used specifically for work purposes), or in paper form, must be kept secure and separate from other files or documents.

Use of AI

Artificial Intelligence technologies (AI) refer to systems or tools capable of performing tasks that typically require human intelligence. These include, but are not limited to, decision-making, natural language processing, image recognition, predictive analytics and automated reasoning. UEL may use AI to support and enhance various processes, including data analysis, decision-making, and automation. We are committed to ensuring that all AI-driven data processing activities comply with the UK GDPR and other relevant data protection laws in the following ways:

i. **Transparency and Fairness**:
When AI is used to process personal data, we strive to ensure that Data Subjects are informed about these processes, including the purposes for which AI is used, our lawful basis for processing personal data using AI, the types of data it analyses, and any potential impact on individuals' rights. We aim to use AI systems in a fair and non-discriminatory manner, actively mitigating any risks of bias.

ii. **Data Minimisation and Accuracy**:
AI processing is conducted with data minimisation in mind, meaning we only process the data that is necessary and proportionate for the intended purpose. We implement robust data quality checks to ensure the accuracy and reliability of AI outputs, especially when these are used in automated decision-making.

iii. **Safeguards and Human Oversight**:
We will restrict automated decision-making (including profiling) on special category

data which results in legal or similarly significant effects. For other personal data, we will implement appropriate technical and organisational measures to safeguard and protect personal data processed by AI, including pseudonymisation, encryption, and access controls. Meaningful human oversight will be in place so that data subjects will have the ability to contest decisions and request human intervention.

iv. **Data Subject Rights**:
Individuals retain all data subject rights concerning AI-driven processing. This includes the right to be informed, the right of access to one's data, the right to rectification.

v. **Ethics and Accountability**:
We are committed to using AI responsibly and ethically. We regularly review our AI systems to assess their impact on privacy and data protection, conducting Data Protection Impact Assessments (DPIAs) in collaboration with the DPO, where necessary and consulting with the Information Commission as required.

vi. **Ongoing Monitoring and Improvement**:
UEL continually monitors the performance and impact of our AI systems, updating them as needed to align with evolving legal standards, ethical guidelines, and technological advancements. Any significant changes to the use of AI will be reflected in this policy, ensuring ongoing compliance with data protection principles.

More information on how Generative AI technologies are utilised in a manner consistent with UEL's values and ethical principles can be found in our Generative Artificial Intelligence Usage Policy.

Publication of UEL Information

As a public authority subject to the Freedom of Information Act 2000, it is the policy of UEL to make public as much information about the institution as possible. In particular, the following personal data will be available to the public for inspection via our website, annual accounts or by submission of a Freedom of Information Request:

- Names of our Board of Governors
- Names and job titles of the University Executive Board
- Salary scales

The disclosure of personal data to third parties under the Freedom of Information Act will be reviewed on a case-by-case basis and must always comply with the data

protection principles described above. However, there may be times that a public interest test could apply and the public interest in disclosing personal data of specific staff outweighs the public interest of withholding said information.

Law Enforcement Requests & Disclosures

In certain circumstances, personal data will be shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of a tax or duty
- By the order of a court or by any rule of law

If UEL or a known third-party processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice a potential investigation. If any UEL employee receives a request from a court or any regulatory or law enforcement authority for information relating to personal data held by UEL, the request must be directed to the Data Protection Officer who will provide comprehensive guidance and assistance.

Data Protection Training

All UEL employees, contractors, temporary staff and volunteers that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training, which will include data protection training. For areas that process high volumes of personal data or special category data, bespoke data protection training is available. All training and awareness can be discussed and requested via the Information Assurance Office or by contacting dpo@uel.ac.uk.

Data Sharing and Transfers

UEL may share or transfer personal data and / or special category data to internal recipients or other organisations (including external third parties such as suppliers) to provide services on our behalf (Data Processors). In some cases, such transfers may take place outside of the EEA (European Economic Area). UEL and its entities will only transfer or share personal data to, or allow access by, third parties when it is assured that the information will be processed lawfully and protected appropriately by the recipient and/or data processor. Processes for data sharing and transfers can be found in Appendix F.

Cookies

A cookie is a small piece of data that a website stores on your device when you visit it, and which is then read when you later revisit the site. The word "cookies" in this Notice and the consent also refers to other forms of automatic collection of data or cookies placed by other software.

Cookies are used to enable certain features (e.g. logging in), to track site usage (e.g. analytics), to store your user settings (e.g. time zone, notification preferences), and to personalise your content (e.g. advertising, language). They may contain information about the website itself, a unique identifier that allows the site to recognise your web browser when you return to the website, additional data that serves the purpose of the cookie, and the lifespan of the cookie itself. For more information about cookies and how UEL uses them, please refer to our Cookies Notice.

Complaints Handling

Data Subjects who wish to complain about the processing of their personal data should first put forward the matter in writing to the Data Protection Officer in the first instance at dpo@uel.ac.uk or for the attention of the Data Protection Officer at University of East London, University Way, London E16 2RD. Complaints will be considered on a case-by-case basis, and where applicable an investigation will be conducted. If the DPO was involved in the processing of the original request which is the subject of the complaint, the investigation will be escalated to, and conducted by an independent UEL representative. The DPO or their nominated representative will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the DPO (or independent representative, where appropriate), the Data Subject can then seek redress through the Information Commission as the Supervisory Authority for the UK . Complaints can be logged via a form: personal-information-complaints-form-new-final-2307.pdf which contains contact details for submitting by email, postal and phone. Further advice can be found at How to make a data protection complaint to an organisation | ICO

**The ICO requires that all data subjects liaise with, and exhaust all avenues for resolution with UEL before a complaint is escalated to them.*

Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft, loss, or exposure of personal data must immediately, or as soon as reasonably possible notify the DPO providing a description of what occurred.

Notification of the incident can be made via e-mail at dpo@uel.ac.uk, by phone, or by using the incident reporting form on the Information Assurance Office intranet pages.

The DPO or an appointed representative will investigate all reported incidents to confirm if a personal data breach has occurred. If confirmed, the DPO will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For severe and high-impact personal data breaches, the DPO will initiate and chair an emergency response team with key individuals to coordinate and manage the personal data breach response (including, but not limited to the University Secretary and Chief Compliance Officer; the Chief Information Officer [for breaches resulting from cyber-attacks and/or IT system failures] and Director of Communications to ensure we are keeping all affected parties up to date with information relating to the breach]). We will also notify the Information Commission and affected Data Subjects, where appropriate.

Research Purposes Exemption

The Data Protection Act 2018 contains specific exemptions for the use and retention of personal data in scientific, statistical or historical research. Personal data collected fairly and lawfully for the purpose of one piece of research can be used for other research purposes, providing that the final results of the research do not identify the individual or adversely affect other individual rights. For example, such data must not be processed in such a way that leads to direct consequences for the individual concerned, or in a way that is likely to cause substantial damage or distress to any Data Subject. Records or questionnaires may be kept in order that the data can be revisited and re-analysed. For further information on data protection in research please email researchethics@uel.ac.uk.

Retention of Data

UEL will keep some forms of information for longer than others, in accordance with legal, financial, archival, or other business requirements. In accordance with the storage limitation principle (UK GDPR principle (e)), UEL will dispose of any personal data for which it no longer has a specified purpose. Further details on how UEL applies consistent retention periods and other controls for the management of records can be found in our Records Management Policy that sets out current retention periods.

CCTV

UEL operates CCTV installations across all campuses comprising of static cameras, body worn cameras and cameras equipped with number plate recognition technology in our carparks. The purposes of the CCTV installations are:

- The protection of staff, students, visitors, and the assets of the University
- The prevention, investigation and detection of crime and disciplinary offences in accordance with the University disciplinary procedures

- The apprehension and prosecution of offenders (including the use of images / data as evidence in criminal / civil proceedings)
- The monitoring of the security of premises

Data Protection Offences

Under the Data Protection Act 2018, it is an offence to:

- Obtain, procure, sell (which includes to disclose, make available, disseminate or transfer), personal data from UEL systems without the university's explicit consent.
- Retain personal data without UEL's consent (this can include retaining outside the scope of your role; or following the end of your employment or any other contract with UEL)
- Alter, destroy or conceal personal data to prevent a legitimate disclosure
- Recklessly re-identify personal data that has been de-identified without the consent of UEL

If there is evidence of an offence under the Data Protection Act 2018, the matter will be subject to an investigation under our disciplinary procedures.

Where it is found that an offence has been committed, sanctions may include dismissal or expulsion.

In some circumstances, we have a legal duty to report offences to the Information Commission.

Appendices

Appendix A – Supporting documents

Fair Processing Notices (aka Privacy Notices) for various audiences can all be found at Data Protection | University of East London:

- Staff
- Prospective students
- Outreach and Access Participant
- Students
- Alumni
- Reporters of Sexual Misconduct and Harassment

UEL staff can also find useful information on their Intranet, within the Information Security Policy, Acceptable Use Policy and Monitoring Policy.

Appendix B - Glossary of terms

Anonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

Consent: Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Data Controller: A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor: A natural or legal person, Public Authority, Agency or other body which processes Personal Data on behalf of a Data Controller.

Data protection: The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.

Data Protection Officer (DPO): The DPO is responsible for informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.

Data Subject: The identified or identifiable Natural (i.e. living) Person to which the data refers.

Encryption: The process of converting information or data into code, to prevent unauthorised access.

Employee: An individual who works part-time or full-time for UEL under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.

Identifiable Natural Person: Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Lawful basis: At least one of these must apply whenever we process personal data:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract an individual has made with us, or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our 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 (note: as a public authority ,we may only apply this legal basis for processing data when it is in addition to and/or specifically separate from the normal performance of our official tasks.)

Personal data: Any information (including opinions and intentions) which relates to a living, identified or identifiable Natural Person (a 'Data Subject').

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed unknowingly or without authorisation

Process, Processed, Processing: Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Operations performed may include:

- Collecting
- Recording
- Organising
- Structuring
- Storing
- Adapting
- Altering
- Retrieving
- Consultation
- Using
- Disclosing by transmission, dissemination or otherwise making available
- Aligning or combining
- Restricting
- Erasing (Deleting)
- Destroying;

Profiling: Any form of automated processing of Personal Data where personal data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. Particularly to analyse or predict certain aspects concerning that natural

person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

Pseudonymisation: Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without additional information (a "key") that allows the data to be re-identified. The additional information should be kept secure.

Special Categories of Data: Personal data pertaining to or revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Data concerning health (includes physical and mental health and the provision of health care services which reveal information about the Data Subject's health status)
- Sex life
- Sexual orientation
- genetic data (e.g. DNA)

Biometric data (includes visual images and fingerprint data)

Supervisory Authority: An independent Public Authority responsible for monitoring the application of the relevant data protection regulation set forth in national law. In the UK the Information Commission acts as the Supervisory Authority.

Third Country: Any country or territory outside the UK. They may or may not have an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the processing of personal data and this should be confirmed before processing within a third country begins.

Third Party: An external organisation with which UEL conducts business and is also authorised to, under the direct authority of UEL, process the personal data under the responsibility of UEL as a Data Controller.

UEL Entity: A UEL establishment, including subsidiaries and joint ventures over which UEL exercise management control.

Appendix C – Examples of personal data

Personal data includes (but is not limited to):

- Staff and student records
- Alumni data
- Applicant data

- Examination marks
- Research data
- Electronic data relating to personal devices, images and audio records
- Residence and catering information
- Details of financial transactions
- Other information about its staff, students and third parties which enables UEL to monitor performance and achievements as well as compliance with health and safety and other legislation

Appendix D – Responsibilities

Senior Management Responsibilities

Each Dean of School or Head of Service is responsible for:

- Ensuring that the personal data held by that School or Service is kept securely and used properly, within the principles of the UK GDPR and Data Protection Act 2018
- Advising the Data Protection Officer or delegated representative of the types of personal data held in their School or Service, and of any changes or new holdings
- Notifying the Data Protection Officer of any instances that could be considered a breach of the legislation
- Ensuring that any advice, guidance or instruction issued by the Data Protection Officer, or delegated authority in terms of data protection compliance are given due consideration and, where appropriate, passed down to team level for action
- Ensuring that all staff or, where appropriate, students receive data protection training
- Ensure that where necessary, staff are provided with resources required to complete mandatory data protection activities including responding to information rights requests and Data Protection Impact Assessments

Staff Responsibilities

All staff process data in one form or other, and are hence responsible for:

- Only processing personal data for the purposes explicitly required for their role;
- Ensuring that data they are responsible for is kept securely and protected against unlawful processing, accidental loss, damage or destruction;
- Attending data protection training
- Reporting known or suspected breaches of data protection to the DPO in the first instance, and their immediate line manager;

- Ensuring that any processing of personal data takes place within the limits of UEL's Fair Processing Notices and complies with our policies, and;
- Notifying the Information Assurance Office if they wish to use an application, system or service that is not supported by IT Services that will involve the processing of personal data

Ensuring that all personal data provided to UEL is accurate and up to date and notify the University promptly about changes to any of their data.

Student Responsibilities

- Students must ensure that all personal data provided to UEL is accurate and up to date. They must also ensure they notify the University promptly about changes to any of their data (such as a change of address);
- Students who use UEL's computing facilities may process personal data as part of their studies. If personal data is processed, students have a responsibility to ensure that all processing is in line with the data protection principles above
- Students who are undertaking research projects using personal data must ensure that:
    - The research has been subject to ethical review and ethical approval has been received
    - All research participants are informed of the nature of the research and are given a copy of UEL's Fair Processing Notice and this Data Protection Policy
    - Where consent of a Data Subject is required for processing, consent must be in writing, freely given, specific, informed, and an unambiguous indication of the Data Subject's wishes
    - The Data Subject understands that consent can be withdrawn at any time
- All information is kept securely using appropriate technical controls – IT Services can be contacted for guidance

Appendix E – Information Rights

The information rights within Data Protection law are

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability

- The right to object
- Rights in relation to automated decision making and profiling

Where an individual makes a request relating to any of the rights listed above:

- UEL will consider each such request in accordance with all applicable Data Protection laws and regulations;
- No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature;
- A response to each request will usually be provided within 30 days of the receipt of the written request from the Data Subject;
- Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative;
- Data Subjects shall have the right to require UEL to correct or supplement erroneous, misleading, outdated, or incomplete personal data.

If the nature of a data request and/or the data to be sourced is of a volume and/or complexity which would not allow UEL to respond fully to the request within 30 days, the DPO shall provide the following information to the Data Subject or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request
- Any information located to date
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision
- An estimated date by which any remaining responses will be provided
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature)
- The name and contact information of the UEL individual who the Data Subject should contact for follow up

Anyone wishing to raise a complaint about the use of their personal data may do so by contacting dpo@uel.ac.uk. UEL will provide a formal response within 30 days of the receipt of the complaint.

Appendix F – Data Sharing and Transfers

UEL will only share personal or special data where one of the scenarios listed below applies:

- The Data Subject has given consent to the proposed transfer or sharing

- The transfer or sharing of data is necessary for the performance of a contract with the Data Subject
- The transfer or sharing is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request
- The transfer or sharing is required to fulfil a statutory legal obligation
- The transfer or sharing is necessary for the conclusion or performance of a contract to be concluded with a third party in the interest of the Data Subject
- The transfer or sharing is legally required on important public interest grounds
- The transfer or sharing is necessary for the establishment, exercise or defence of legal claims
- The transfer or sharing is necessary to protect the vital interests of the Data Subject

In all cases, such transfers will be subject to appropriate safeguards and will only occur when evidence of such safeguards has been provided. Examples of such safeguards include an information sharing agreement or contractual clauses that legally oblige the recipient to respect data protection law.