Data Protection Policy

General Data Protection Regulation (EU) 2016/679 & Data Protection Act 2018

Summary

- The Data Protection Act 1998 is being replaced by the Data Protection Act 2018, which is based on the General Data Protection Regulation

- The new law applies to data that can identify a person – personal data.

- Some data is particularly sensitive such as ethnicity or medical data; this is considered 'special category' data.

- This policy explains how the University meets its obligations under the Data Protection Act, outlines the **responsibilities of staff and students** and provides information on the information rights associated with how personal data is managed. Complying with this policy is a condition of employment or study at UEL.

- This policy forms part of the wider Data Protection Framework that has designed to ensure ongoing compliance with Data Protection law and the implementation of data protection best practices across the institution.

- UEL has a legal obligation to only process personal data in line with the data protection principles

- UEL must also provide information about any processing of personal data taking place and ensure that individuals are aware of and can exercise their information rights.

- Individuals about whom personal data is being processed have rights concerning how their personal data is managed.

- All staff, students and third parties associated with UEL have a responsibility to ensure that they keep personal data secure, only share it when authorised to do so and only use personal data for the purpose it was collected.

- Any students that process the personal data of others as part of their course are subject the same stipulation and to the relevant points in this policy.

- In the event of a data breach or a suspected breach, staff and students have a responsibility to notify the Data Protection Officer or appropriate member of staff as soon as possible.

- Misuse of data or negligent disregard for the obligations contained within the Data Protection Act, are criminal offences.

- Any queries relating to the privacy policy, or any concerns relating to data protection at UEL should be sent to dpo@uel.ac.uk in the first instance.

Full Policy Wording

Introduction

The University of East London (UEL) is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. The General Data Protection Regulation (EU) 2016/679 (GDPR) replaces the Data Protection Act (1998) in law from the 25th May 2018. The new legislation will be implemented in the UK by way of the Data Protection Act 2018 (the Act.) This policy will be updated to reflect these changes.

The purpose of this Policy is to outline the roles and responsibilities that every current employee, enrolled, prospective or former student and all data processors must comply with to ensure they abide by the law by ensuring the confidentiality, integrity and security of any personal data held or shared by UEL, whatever the medium.

This policy forms a core part of UEL's Data Protection Framework, which has been designed to reduce privacy risk and help the University implement a Personal Information Management System to ensure ongoing compliance with Data Protection Law and embed data protection best practice throughout the institution.

The GDPR and the Data Protection Act (2018) contain familiar elements from the 1998 legislation such as the Data Protection Principles of Good Practice and specific rights for individuals with regards to how their personal data is processed. However, the GDPR imposes additional requirements, which are reflected in the new legislation.

Like the 1998 Act, the 2018 Act applies to 'personal data'. Personal data is **any** information (including opinions and intentions) which relates directly or indirectly to an identified or identifiable living person. Some types of data are particularly sensitive. Sensitive data includes information such as genetic, biometric or medical/health data, information concerning race, sexual orientation religious or political beliefs and trade union membership. This type of data is special category data and must be treated particularly carefully.

Under the 2018 Act, personal data and special category data are subject to a number of new legal safeguards and other regulations, which impose restrictions on how organisations may process personal data within their organisation. An organisation that handles personal data and makes decisions about its use is a Data Controller. As a Data Controller, UEL is responsible for ensuring compliance with the Data

Protection requirements outlined in this Policy. Non-compliance may expose UEL to complaints, regulatory action, fines and/or reputational damage.

UEL is fully committed to ensuring continued and effective implementation of this Policy, and expects all UEL employees, students, associates third parties and processors to share in this commitment. Any breach of this Policy is taken seriously and may result in disciplinary action or business sanction.

For a full list of definitions, please see Appendix A.

Scope

This policy applies to any individual or organisation that processes personal data for or on behalf of UEL or business affiliated to UEL activities. Processing of personal data includes but is not limited to the identification, collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure by any means, restriction, erasure or destruction of personal data.

This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing 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 is designed to establish a worldwide baseline standard for the processing and protection of personal data by all UEL entities. Where national law imposes a requirement which is stricter than imposed by this Policy, the requirements in national law must be followed. Where national law imposes a requirement that is not addressed in this Policy, the relevant national law must be adhered to.

If there are conflicting requirements in this policy and national law, please consult with Governance and Legal Services for guidance.

Purpose and Principles of Data Collection and Processing

UEL needs to collect and store a wide range of personal data and special category data about its employees, students and other users of UEL facilities to allow it to maintain its core operations.

Personal data includes 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, and details of financial transactions. Other information about its staff, students and affiliates

enables UEL to monitor its performance and achievements, and compliance with health and safety and other legislation.

To comply with the Act, UEL must:

- Be accountable and transparent in how and why it uses personal data
- Demonstrate compliance with the data protection principles
- Allow a person to exercise their Information Rights
- Adhere to approved codes of conduct for data protection

Data Protection Principles

UEL has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Lawfulness, Fairness and Transparency - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
Purpose Limitation - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data Minimisation - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
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 for the purposes for which the personal data is processed.
Integrity & Confidentiality - Personal data shall 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.
Accountability principle - UEL must demonstrate that the six Data Protection Principles are met for all personal data for which it is responsible.

Every person associated with UEL who processes or uses any personal data must abide by these Principles at all times. In order to ensure that this happens, UEL has developed this Data Protection Policy.

Responsibilities

The Act mandates that the data controller will be responsible for ensuring that personal and special category data are collected, stored and processed fairly, for deciding which types of information will be processed and the reason for the Processing. The legal responsibility of data controller rests with UEL Higher Education Corporation, and the Board of Governors, as UEL's governing body, is ultimately responsible for implementation.

The Board of Governors has allocated the responsibility for the protection of personal data at Senior Management level to a Data Protection Officer (DPO) who is authorised to act independently and has overall responsibility for ensuring ongoing compliance with UEL's data protection obligations. The role of the DPO is autonomous and the person that fulfils this role within UEL reports to the highest level of management within the organisation. The DPO is also the first point of contact for Supervisory Authorities and for individuals whose data is processed.

Senior Management Responsibilities

Each Senior Manager is responsible for:

- Ensuring that the personal data held by that College or service is kept securely and used properly, within the principles of the GDPR;
- Advising the DPO of the types of personal data held in their school or service, and of any changes or new holdings;
- Notifying the DPO of any instances that could be considered a breach of the Act and;
- Ensuring that any advice, guidance or instruction issued by the DPO in terms of data protection compliance are given due consideration.

Where processing of personal data will involve new technology or high-risk activities such as sensitive research a Data Privacy Impact Assessment may need to be conducted. The DPO will act as the authority in this work and will advise Deans and Directors of when and how such work is to be completed.

Staff Responsibilities

All staff are responsible for:

- Checking that the information that they provide in connection with their employment is accurate and up-to-date.

- Informing HR Services of any changes to information that they have provided i.e. changes of address, or of any errors.
- Checking that any statements made by UEL from time to time about the kind of data kept on staff and students are accurate and up-to-date.
- Ensuring that if they process personal data as part of their role they attend data protection training when directed;
- Reporting known or suspected breaches of data protection to their immediate line manager;
- Ensuring that any Processing of personal data takes place within the limits of UEL's Fair Processing Notice

Student Responsibilities

Students must ensure that all personal data provided to UEL is accurate and up-to-date. They must ensure that changes of address etc. are notified to the Student Services and to their school.

Students who use UEL's computing facilities may process personal data as part of their studies. If the Processing of personal data takes place, students must take responsibility for that Processing activity to ensure that it in line with the data protection principles above.

Students who are undertaking research projects using personal data must ensure that:

- The research subject is informed of the nature of the research and is given a copy of UEL's Fair Processing Notice and this Data Protection Policy.
- Where consent of a Data Subject is required for Processing that the consent is freely given, specific, informed, and unambiguous indication of the Data Subject's wishes
- The Data Subject understands that consent can be withdrawn at any time.
- The Dean of School is informed of the proposed research before it begins, and ensures that UEL is authorised to undertake this kind of research.
- All information is kept securely using appropriate technical controls – Contact IT Services for guidance.

Information Rights

All staff, students and other users about whom UEL process personal data have rights associated with its use. These rights 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 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 UEL cannot 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.

Fair Processing Notices

Where UEL act as a data controller, we will provide information to Data Subjects about how UEL processes personal data and our purposes for processing personal data. We will also identify the circumstances under which transfers take place and provide information about routine disclosures to other data controllers. UEL Fair Processing Notices provide this information for all Data Subjects associated with UEL. A complete list of all of UEL's Fair Processing Notices is publicly available on uel.ac.uk via the privacy section of the website.

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 an 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 Security

All staff and students are responsible for ensuring that:

- Any personal data which they hold in whatever format is kept securely;
- Personal information is not disclosed either orally, in writing, electronically either accidentally or otherwise to any unauthorised third party;
- Personal data that is taken off site is not left unattended or unsecured;
- Desks are kept clear of personal data when unattended;

Where personal information exists in a manual form, it should be kept in a locked filing cabinet or locked drawer. Where personal information is held in an electronic form, each Dean of School, Director of Service is responsible for ensuring that appropriate technical and organisational measures are taken within the school, service or unit to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, such data.

Examples of such measures include encryption, both at rest and in transit, anonymization and pseudonymising. Each Dean of School or Director of Service is responsible for promoting data protection of best practice within their teams and keeping the DPO informed of changes in the collection, use, and security measures used for personal data within the school, service or unit.

Publication of UEL Information

Information that is already in the public domain is exempt from the Data Protection legislation in some cases.

It is the policy of UEL to make public as much information about UEL as possible. In particular, the following information will be available to the public for inspection:

- Names of Officers of UEL;
- Members of the Board of Governors;
- Staff lists and areas of expertise;

The UEL internal telephone directory is not a public document.

Any individual having good reason for wishing details in these categories to remain confidential should advise the DPO who will consult with the University Secretary.

Subject Consent to the Processing of Special Category Information

In some cases, UEL can process personal data only with the consent of the individual or, if the data are sensitive, explicit consent must be obtained. From the date that this policy takes effect, concerns or questions relating to consent should be addressed to the DPO in the first instance. Agreement to UEL processing some specified classes of personal data or special category data is a condition of acceptance of a student on to any course, and a condition of employment for staff whether permanent or on a contracting basis.

Some posts or programs of study will bring applicants into contact with children, including young people of any age but in any case under 18. UEL has a duty under the Children Acts and other legislation to ensure that staff are suitable for the post, and students for the programs offered. UEL also has a duty of care to all staff and students and must therefore make sure that employees and those who use University facilities do not pose a threat or danger to other individuals.

UEL may ask for information about a person's health, particular health needs such as allergies, or any conditions such as asthma or diabetes. UEL will only use such information in the protection of the health and safety of the individual. UEL may also ask for information about a person's criminal convictions, race, gender and family details. This is to ensure that UEL is a safe place for everyone, or may be to operate other UEL policies, such as the sick pay Policy or the equality and diversity Policy.

Data Protection Training

All UEL employees 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 a data protection e-learning course. For areas that process high volumes of personal data or special category data, bespoke data protection training can be offered. All UEL staff and students have access to a dedicated data protection intranet site that outlines key responsibilities.

Data Sharing and Transfers

UEL may share or transfer personal data or special category data to internal recipients or other organisations known as Data Processors. In some cases such transfers may take place outside of the EU.

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 defense of legal claims.
- The transfer or sharing is necessary in order to protect the vital interests of the Data Subject.

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 legitimately and protected appropriately by the recipient and/or data processor. Where third party processing takes place, the department arranging the transfer will first identify if the third party is considered a Data Controller or a Data Processor of the personal data to be transferred. Where the third party is deemed to be a Data Controller, UEL will enter into, in cooperation with the DPO, an appropriate agreement with the third party to clarify each party's responsibilities in respect to the personal data transferred.

Where the third party is deemed to be a Data Processor, UEL will enter into, in cooperation with the DPO, an adequate processing agreement with the Data Processor. The agreement will require the Data Processor

to protect the personal data from further disclosure and to only process personal data in compliance with UEL instructions. All processing of personal data by a Data Processor acting on behalf of UEL must be documented and new processing activities that involve personal data or special category data should be notified to the DPO who will ensure that the relevant contractual clauses are made available before processing commences.

Complaints Handling

Data Subjects with a complaint about the processing of their personal data should put forward the matter in writing to the University's Complaints Team. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The DPO or a 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 DPO, or appointed representative, then the Data Subject may, at their own cost, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction. Further information on the complaints process can be provided by Governance & Legal Services.

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 notify the DPO providing a description of what occurred. Notification of the incident can be made via e-mail dpo@uel.ac.uk, by phone, or by using the incident reporting form at uel.ac.uk.

The DPO or an appointed representative will investigate all reported incidents to confirm if a personal data beach 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 personal data breaches, the DPO will initiate and chair an emergency response team to coordinate and manage the personal data breach response including notifying the relevant Supervisory Authority if appropriate.

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, UEL will dispose of any personal data for which it no longer has a specified purpose.

Research Purposes Exemption

Data collected fairly and lawfully for the purpose of one piece of research can be used for other research, providing that the final results of the research do not identify the individual. Such data must not be processed to support measures of decisions with 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 reanalysed. This exemption is only applicable to academic research, and cannot be used to provide information about an individual.

CCTV & Monitoring

UEL operates a number of CCTV installations that comprise of fixed cameras, printers, monitors, signs, recording and playing equipment, information, material, data, and any ancillary equipment required for the operation of the installations (e.g. cabling, printers, power supplies).

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.

The University's CCTV installations will be registered under UEL's Data Controller registration with the ICO and all release of information will be in accordance with the registration.

An exemption to the provisions of the Data Protection Act 2018 covers the disclosure of information for the purposes of:

- Preventing or detecting crime
- Apprehending or prosecuting offenders
- Assessing or collecting any tax or duty

This exemption applies only where non-disclosure would be likely to prejudice one of these purposes. For further information on the use of CCTV please contact Estates & Facilities. In addition to the use of CCTV UEL also utilises other monitoring technologies including the use of Automatic Number plate Recognition (ANPR), email and system scanning and logging processes. For further information, please see UEL's Monitoring policy.

Annex A

Definitions

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 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.

Personal data: Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person or 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:

- collection;
- recording;
- organisation;
- structuring;
- storage;
- adaptation;
- alteration;
- retrieval;
- consultation;
- use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination;
- restriction;
- erasure;
- destruction.

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. In particular 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 a "key" that allows the data to be re-identified.

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 or sex life and sexual orientation; genetic data or biometric data.

Supervisory Authority: An independent Public Authority responsible for monitoring the application of the relevant data protection regulation set forth in national law.

Third Country: Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

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.

Version Control

Document Version Number	**1.0**
Document Owner	**Data Protection Officer – Vice Chancellors Group**
Document Approved By	**Vice Chancellors Group**
Approval Date	**18th March 2018**
Review Date	**This policy may be amended to reflect changes in the Data Protection Bill that occur when the Bill receives Royal Assent prior to becoming the Data Protection Act 2018.**