Information Assurance Office

University of East London

Pioneering Futures Since 1898

Data Protection Policy

Version control							
Version No.	**Date**	**Equality analyses completed**	**Responsible Officer**	**Last review**	**Next review**	**Approved by**	**Date of approval**
2	**July 2020**	**Yes**	**Data Protection Officer**	**July 2020**	**July 2021**	**UEB**	**15 July 2020**

Information Assurance Office

University of East London

Pioneering Futures Since 1898

Table of Contents

Information Assurance Office

University of East London
Pioneering Futures Since 1898

Data Protection Policy

Summary

- This policy applies to any data that could identify an individual either directly or in combination with other data that you may hold or come into possession of this is known as **personal data**.

- 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 how and why we process special category data can be found in our Sensitive Data Policy.

- Complying with this policy is a condition of employment or study at UEL. Non-compliance with the obligations within this policy may result in disciplinary action.

- Misuse of data or negligent disregard for the obligations contained within the Data Protection Act, or any law designed to protect personal data, could lead to prosecution and a criminal record.

- This policy explains how the University meets its obligations under the Data Protection Act 2018 and outlines the responsibilities of staff and students when they collect, use or process personal data.

- This policy forms part of UEL's Information Governance Framework that has been designed to ensure ongoing compliance with Data Protection and other information laws and the implementation of information governance best practices across the institution.

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

- 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, 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 conditions and to the relevant points in this policy.

- Personal data processed for UEL purposes on personal devices is still subject to the

obligations of 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 data protection principles.

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

- 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.

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

Scope

This policy applies to any individual or organisation that processes personal data for, or on behalf of, the University of East London or another business affiliated with our activities.

Processing of personal data occurs when an action is carried out on the personal data to complete a function. Processing activities include but are not limited to the identification, collection, recording, organising, 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, 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 establishes 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 the Governance and Legal team for guidance.

Purpose of Data Collection and Processing

UEL needs to 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:

- 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, destruction or damage.

Information Assurance Office

University of East London
Pioneering Futures Since 1898

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 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 and in a transparent manner;

- **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, 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, destruction or damage to that data;

- **Accountability -** 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 is also the first point of contact for Supervisory Authorities and for individuals whose data is processed.

Each Dean of School or Director of Service is responsible for promoting and modelling best practice 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 the School, Service or unit. To meet this requirement, the Information Assurance Office will train Univeristy staff to act as Data Protection Advisors responsible for promoting best practices and reporting issues within their own departments. Senior Management, staff and students all have responsibilities in relation to data protection, which are highlighted in Appendix C.

Where processing of personal or special category data will involve new technology or high-risk activities such as a high degree of monitoring or profiling, a Data Privacy Impact Assessment may need to be conducted. A Data Protection Impact Assessment template has been produced by the Information Assurance Office and advice and guidance is available on the Intranet site. Business Owners are responsible for ensuring that any risks identified in a Data Protection Impact Assessment are mitigated to a level that falls within the institutional risk appetite.

Information Rights

Every person about whom UEL process 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 in complying with our obligations around responding to information rights requests.

A breakdown of these rights and the process for putting in a request relating to information rights, is listed in Appendix D.

Fair Processing Notices

Where UEL acts as a Data Controller, we will provide information about how UEL processes the personal data of data subjects and our purposes for processing that 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 on uel.ac.uk via the Data Protection section of the website.

Information Assurance Office

University of East London
Pioneering Futures Since 1898

Information Security

All staff and students are responsible for ensuring that:

- Any personal data which they hold in whatever format is kept securely;
- Personal data is not disclosed either orally, in writing or 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, drawer or in a secured area.

Where personal data is held in an electronic form, each Dean of School or Director of Service is responsible for ensuring that appropriate technical and organisational measures are taken to ensure against unauthorised or unlawful processing of personal data and against accidental loss/ destruction of/damage to such data. This includes data that is held by a third party such as a cloud services provider. See Recommended Software and Systems for more information.

Examples of such measures include:

- Encryption of personal data in transit and at rest;
- Secure retention or disposal of personal data in a timely fashion;
- Limiting access as necessary and proportionate for the purpose;
- Ensuring that the system meets the technical requirements needed to fulfil any type of Information Rights request;
- Where held internally the data is held on UEL SharePoint, or within the UEL Office 365 environment;
- Where held by a Data Processor or third party, the data is located within the European Union and
- Limiting the sharing of data to what is proportionate and necessary to achieve the purposes.

Use of UEL Email

The use of the UEL email system should be used to communicate UEL business in line with our Email policy. The use of personal email addresses for UEL business for staff and students is not permitted where access to UEL email systems is available. While the use of email attachments is permitted for general business, documents containing personal or special category data should be shared using SharePoint, OneDrive for Business or Microsoft Teams. When sending personal data externally,

SharePoint should be used where available. As an alternative, documents can be password protected and sent as an email attachment.

Remote Working

When working remotely, the principles and obligations of the Data Protection Act 2018 still apply. All staff are expected to ensure that any data they process from home (including on their own personal devices or in paper form) is kept secure and separate from other files or documents.

The data in certain applications such as Office 365 will be protected using multi-factor authentication and other measures including the encryption of data and the potential restriction of downloading and sharing functionalities.

When using personal equipment such as laptops, staff are expected to ensure that software is kept up to date and anti-virus software is installed. Where you need to share data, staff must use their UEL email, Microsoft Teams, OneDrive or SharePoint accounts. The sharing of UEL data using personal email addresses or personal cloud storage or communications platforms is not permitted.

Recommended Software and Systems

IT Services and CELT offer and support a range of systems, applications and services to meet the core business purposes of the University. These supported systems have been assessed to ensure that they meet our requirements on functionality, storage of data, disaster recovery, security and regulatory compliance with data protection and other relevant laws. Any staff or students that wish to use applications, software or services that are not recommended by IT Services or CELT are responsible for ensuring that appropriate controls are in place to allow UEL to comply with the obligations of the Data Protection Act and other relevant laws. Due to the complex nature of compliance, it is strongly recommended that you check with IT Services and CELT before using new systems, apps or services.

The Information Assurance Office will assist in assessing compliance where appropriate however you must notify the Information Assurance Office or delegated representative that an assessment of an unsupported application, system or service is required **before** personal data is processed.

Where use of an unsupported system, application or service is deemed to create a risk to the university, the Data Protection Officer or delegated representative will present these risks, along with proposed steps to mitigate them. If you choose not to implement the suggested mitigations and accept the level of risk, the Information Assurance Office will seek acceptance of these risks using a Risk Acceptance Form signed by the appropriate Dean or Director of Service which will be kept under regular review.

In cases where there is potential of such systems, applications or services to breach our obligations around data protection (e.g. not comply with the data protection principles) the Data Protection Officer has a legal obligation to highlight this potential breach to the relevant Deans or Directors and if necessary, the University Executive Board and / or the Information Commissioners Office. Such breaches place a legal obligation on UEL to stop processing the personal data in a way that breaks the law and, in such cases, immediate steps will be taken by the Information Assurance Office to ensure the university remains compliant with its obligations.

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 Officers of UEL;
- Names of our Board of Governors;
- Names and job titles of the University Executive Board;
- Names and job titles of members of the University Management Board;
- Staff lists and areas of expertise - the UEL internal telephone directory is not a public document.
- Names and job titles of senior staff.

If an individual wishes any details, in the categories listed above, to be confidential and has good reason for this, they must contact the DPO who will consult with the University Secretary. 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.

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. Further details on how we will handle disclosures can be found in our Confidentiality and Disclosure policy.

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 UEL staff and students have access to a dedicated data protection intranet site that outlines key responsibilities and contains resources for ensuing that we can demonstrate compliance.

Data Sharing and Transfers

UEL may share or transfer personal data or special category data to internal recipients or other organisations to provide services on our behalf (Data Processors). In some cases, such transfers may take place outside of the EU. 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. Processes for data sharing and transfers can be found in Appendix E.

Complaints Handling

Data Subjects with a complaint about the processing of their personal data should put forward the matter in writing to the Information Assurance Office in the first instance. Complaints will be considered on a case by case basis, and where applicable an investigation will be conducted. 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 Supervisory Authority within the applicable jurisdiction. In the United Kingdom, the Information Commissioners Office acts as an independent regulator for this purpose.

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 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 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.

Research Purposes Exemption

The Data Protection Act 2018 contains specific exemptions for the use 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, providing that the final results of the research do not identify the individual. 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. This exemption is only applicable to academic research and cannot be used for commercial, or market research purposes. 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, UEL will dispose of any personal data for which it no longer has a specified purpose. In order apply consistent retention periods to our most commonly collected data, we have produced a Records Retention Schedule 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.

Monitoring of networks and accounts

The University takes a range of proactive measures to protect personal data, its technology, infrastructure, computer networks and intellectual property. Every user of our network is issued with a unique username and password to their own user account. Any actions taken on this account are logged and can be audited by IT Services. This includes but is not limited to:

- Any websites visited while logged in to your UEL account;
- Any email that is sent or received by your UEL email address and
- Any instant messages sent or received by Microsoft Teams.

The University utilises Data Loss Prevention technology to reduce the risk of high volumes of personal data leaving our network via any Office 365 pathway including by email, OneDrive for Business or SharePoint. Where we get an alert that such activity has taken place, our Information Security team along with the Information Assurance Office will investigate to ensure that the disclosure of personal data remains compliant with information law. More information about our monitoring activities can be found in our Monitoring policy.

Data Protection Offences

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

- Obtain, disclose, sell or offer to sell personal data from UEL systems without the consent of UEL; Retain personal data outside the scope of your role or following the end of your employment without the consent of 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 Information Commissioners Office.

Appendix 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. 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 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. In the UK the Information Commissioners Office acts as a Supervisory Authority.

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.

Appendix B – Examples of personal data

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
- Details of financial transactions.
- Other information about its staff, students and affiliates which enables UEL to monitor performance and achievements as well as compliance with health and safety and other legislation.

Appendix C – 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 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 and;

- 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 are 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 if any part of their role could involve processing personal data.

- 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 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.

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 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, 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 D – 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 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.

Appendix E – 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 have been provided. Examples of such safeguards include an information sharing agreement or contractual clauses that legally oblige the recipient to respect data protection law.

Third party processing

Where third party processing takes place, the department wanting to share personal data with a Data Processor or other party is responsible for ensuring that the Information Assurance Office are aware

of the requirements and for implementing any specific measures required to make the sharing lawful and secure.

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 are legally required to enter into a contract for the processing of the personal data.

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 the DPO should be notified about any new processing activities that involve personal data or special category data.

This ensures that the relevant contractual clauses are made available before processing commences.