DATA PROTECTION POLICY

Originator	Data Protection Officer
Date	January 2024
Approved by	SMT
Document Type	Policy
Previous Version	March 2021

CONTENTS

1. Introduction

1.1 Leeds Arts University ("the University", "we" or "our") obtains, uses, stores and otherwise processes Personal Data relating to potential staff and students (applicants), current staff and students, former staff and students, current and former workers, contractors, website users and contacts (Data Subjects). When Processing their Personal Data, the University is obliged to fulfil individuals' reasonable expectations of privacy by complying with relevant Data Protection Legislation, including the UK GDPR as amended, the EU GDPR and the Data Protection Act 2018.

1.2 This Data Protection Policy sets out how we will handle the Personal Data of our Data Subjects. This policy applies to all data Processing activities of the University, and is applicable to staff whether permanent or temporary, contractors and others employed under a contract of service ("Staff" or "you"). You must read, understand and comply with this policy when Processing Personal Data on our behalf and attend training on its requirements. Data protection is the responsibility of everyone within the University and this policy sets out what we expect from you when handling Personal Data to enable us to comply with Data Protection Legislation and other applicable law. Related Policies are available to help you interpret and act in accordance with this policy. You must also comply with all those Related Policies.

- We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR, which require Personal Data to be:
    - Obtained and processed fairly and lawfully and in a transparent manner (lawfulness, fairness and transparency);
    - Obtained only for specified, explicit and legitimate purposes (purpose limitation);
    - Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);
    - Accurate and where necessary kept up to date (accuracy);
    - Not kept in a form that permits identification of Data Subjects for longer than is necessary for that purpose (storage limitation);
    - Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);
    - Not transferred to another country without appropriate safeguards in place (transfer limitation); and
    - Made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subjects' rights and requests).

1.3 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in a manner incompatible with those purposes.

1.4 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary. Please contact the Data Protection Officer (DPO) for further information should you wish to use Personal Data for a reason that is different from, or incompatible with, the purpose for which it was originally collected.

2. Status of the Policy

2.1 This policy applies to all Personal Data we Process, regardless of the media on which that data is stored or regardless of who the Data Subject is.

2.2 The University is responsible for and must be able to demonstrate compliance with the data protection principles listed in 1.2 (accountability). In order to support the University's demonstration of accountability, all staff are responsible for data protection within their own roles and data Processing activities.

2.3 It is a condition of employment that employees will abide by the rules and policies made by the University, and your compliance with this policy is mandatory. Any breach of this policy can therefore result in disciplinary proceedings.

3. Notification of Data Held and Processed

3.1 Whenever we collect Personal Data directly from Data Subjects, for example for the recruitment and employment of staff and for the recruitment and enrolment of students, we will provide these Data Subjects with all the information required by the UK GDPR. This includes the identity of the Controller and DPO, and how and why we will use, Process, disclose, protect and retain that Personal Data.

When Personal Data is collected indirectly (for example, from a third party such as UCAS), we will also check that the Personal Data was collected by the third party in accordance with the Data Protection Legislation and on a basis which considers our proposed processing of that Personal Data.

3.2 The University will provide all staff, students and other relevant Data Subjects with a Privacy Notice. This will state all the types of data we hold and Process about them, where it was sourced from, the reasons for which it is processed and for how long we will hold it.

3.3 If you are collecting Personal Data from a Data Subject, directly or indirectly, then a Privacy Notice must be provided to the Data Subject. If our existing Privacy Notices do not cover your proposed activity, then please get in touch with the DPO to discuss drafting an appropriate notice for the Processing.

4. Responsibilities of Staff

4.1 All Staff are responsible for complying with this policy. Line managers are responsible for ensuring that staff within their area of responsibility comply with this policy.

4.2 All Staff have a responsibility to comply with Data Protection Legislation and we will provide data privacy-related training to enable this, which must be undertaken to the schedule outlined. Line managers are responsible for ensuring that staff within their area of responsibility complete the training to the schedule outlined.

4.3 The Data Protection Officer (DPO) is responsible for overseeing this policy and for developing related policies and privacy guidelines. The University's DPO is Katie Machin, ext. 8280, dpo@leeds-art.ac.uk.

4.4 You should contact the DPO if you have any questions about the operation of this policy, the application of Data Protection Legislation, or if you have any concerns that this policy is not being followed. In particular, you should contact the DPO if/whenever:

- You are unsure of the lawful basis on which you are relying to Process Personal Data (see paragraph 5);
- You need to rely on, or capture, Consent (see paragraph 9);
- You need to discuss amendments to, or drafting of new, Privacy Notices (see paragraph 3);

- You are unsure about the retention period for the Personal Data being Processed (see paragraph 14);
- You are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 6);
- There has been a Personal Data Breach (see paragraph 12);
- You are considering transferring Personal Data outside the UK (see paragraph 13);
- A Data Subject has made contact regarding invoking their rights under Data Protection Legislation (see paragraph 8);
- You are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA, or plan to use Personal Data for purposes other than for which it was collected (see paragraph 10);
- You need help complying with applicable law when carrying our direct marketing activities (see paragraph 15);
- You need help with any contracts or other areas in relation to sharing Personal Data with third parties (such as overseas partners, agents, and organisations conducting surveys on the University's behalf) (see paragraph 16).

4.5 All staff are responsible for:

- Checking that any information that they provide to the University in connection with their employment is accurate and up to date.
- Informing the University of any changes to information which they have provided i.e. changes of address.
- Informing the University of any errors or changes. The University cannot be held responsible for any errors unless the staff member has informed the University of them.

4.6 Staff should only process Personal Data when performing their duties requires it and should not Process Personal Data for any reason unrelated to their job duties. Personal Data should only be collected when required, and excessive data should not be collected.

4.7 Designated staff are responsible for ensuring that when Personal Data is no longer needed it is deleted or anonymised in accordance with the University's Records Retention Schedule. In order to keep the University compliant with this Schedule, Personal Data is to be reviewed regularly and deletion and/or anonymisation of that data undertaken routinely.

4.8 The accuracy of Personal Data held must be checked at regular intervals. If Personal Data is inaccurate, it must be corrected or deleted without delay.

5. Lawfulness, fairness and transparency

5.1 Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 You may only collect, Process and share Personal Data for specified purposes, and in accordance with the requirements of 5.1. The UK GDPR restricts actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.3 The UK GDPR allows Processing for specific purposes, known as the legal bases for Processing. The bases that may be considered and used by the University are:

- The Data Subject has given their Consent;
- The Processing is necessary for the performance of a contract with the Data Subject;
- To meet our legal compliance obligations;
- The Processing is necessary for the performance of a task in the public interest;
- To pursue our legitimate interests (or those of a third party)
- To protect the Data Subject's vital interests;

6. Data Security

6.1 Staff are responsible for protecting the Personal Data that we hold. Staff must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Staff must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

6.2 Staff must follow all procedures and technologies that are put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures, and who agree to put adequate measures in place, as requested. If you intend on transferring Personal Data to a new third-party service provider, you must first consult with the DPO (see paragraph 15).

6.3 Staff must maintain data security by protecting the Confidentiality, Integrity and Availability of the Personal Data, as defined in the Glossary.

6.4 Staff must comply with all applicable aspects of our Staff Computer Use Security Policy.

6.5 Staff should note that unauthorised disclosure and/or failure to adhere to the requirements set out in 6.6 to 6.11 inclusive below will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

6.6 Most Personal Data Processed by the University is done so digitally. Computerised and/or portable methods of Processing Personal Data must be done so using password protected technologies. In the limited instances where Personal Data is Processed in paper format, it should be kept in a locked filing cabinet or locked drawer.

6.7 It is recommended that wherever possible Staff do not share Personal Data by email, but instead consider sharing documents and data via Office 365 or by saving the data in an access controlled Network folder.

6.8 When working remotely, Staff should follow internal procedures and guidance on doing so securely, including through accessing University systems via VPN. Wherever possible and practical, Staff should Process Personal Data directly on University systems, rather than processing them locally on laptops and other portable media. Personal Data should not be stored in paper-copy form at Staff members' homes. The security guidelines given in this Policy continue to apply for all Processing of Personal Data controlled by Leeds Arts University, regardless of the location, and must be adhered to.

6.9 Data stored and Processed on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:

- Suitable backups of the data exist;
- Special Categories of Personal Data are appropriately encrypted;

- Special Categories of Personal Data are not copied onto portable storage devices without first consulting a designated data controller or the DPO, in regard to appropriate encryption and protection measures;
- Electronic devices such as laptops, mobile devices and computer media (e.g. USB devices) that contain Special Category Personal Data are not left unattended when offsite.

6.10 Staff should be aware that CDs generally cannot have their data deleted, so writing personal data onto them should always be avoided unless absolutely necessary. USB storage can have data deleted from it, but this can in some cases be recoverable. It is recommended that before disposal all USB storage devices are reformatted to ensure that data cannot be recovered, or that the device is handed to IT who will be able to dispose of it securely.

6.11 For Personal Data which is considered particularly sensitive, the risks of failure to provide adequate security may be so high that it should never be taken home, or Processed locally on a laptop or other portable media. This might include Special Category Personal Data, payroll information, addresses of students and staff, disciplinary or appraisal records or bank account details. This Personal Data should only be Processed remotely when directly accessing University systems, for example via VPN. Exceptions to this may only be with the explicit agreement of a designated data controller or the DPO (see 10).

7. Data Subjects' Rights

7.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- Withdraw Consent to Processing at any time (where the legal basis of Processing is Consent);
- Receive certain information about the Processing activity;
- Request access to the Personal Data that we hold (including receiving a copy of their Personal Data);
- Prevent our use of their Personal Data for direct marketing purposes;
- Ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed, or to rectify inaccurate data or to complete incomplete data;
- Restrict Processing in specific circumstances;
- Object to Processing which has been justified on the basis of our legitimate interest or in the public interest;
- Request a copy of an agreement under which Personal Data is transferred outside of the UK;
- Object to decisions based solely on Automated Processing, including profiling (ADM);
- Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- Make a complaint to the supervisory authority;
- In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

7.2 The identity of any individual seeking to exercise any of their rights under 8.1 must be properly verified before any action is made. Staff must not respond directly, and any requests must be immediately forwarded to the DPO who will be able to advise and/or respond to the request.

7.3 A Data Subject may wish to receive notification of the information currently being held by the University, and receive a copy of that data (known as a Subject Access Request). We aim

to comply with these requests for access to Personal Data as quickly as possible, but will ensure that it is provided within one month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the Data Subject making the request.

7.4 Where a Data Subject has requested their Personal Data to be rectified or erased, we will inform them that their request has been complied with within one month, unless the request is being refused for legitimate reasons, or it is impossible or significantly onerous to do so. In these cases, we will let the Data Subject know as soon as possible, and by no later than one month of receipt of their request.

8. Consent

8.1 A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent typically requires affirmative action. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

8.2 A Data Subject must be easily able to withdraw Consent to Processing at any time (when Consent is the legal basis for Processing), and withdrawal must be promptly honoured. Consent needs to be separately sought if we intend to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first Consented.

8.3 When Processing Special Category Data or Criminal Convictions Data, for example to ensure the University is a safe place for everyone, or to operate other policies and procedures, such as the Absence Notification Procedure and Sick Pay Scheme or Equality, Diversity and Inclusion Policy, we will usually rely on a legal basis other than Consent if possible. Where Consent is used, it will be specifically sought from the Data Subject.

8.4 A record of Consents captured must be recorded and maintained. Heads of business areas that collect Consent are responsible for ensuring that these records are maintained and kept up to date.

9. Privacy by Design and Default and Data Protection Impact Assessments (DPIAs)

9.1 We will implement Privacy-by-Design measures when processing Personal Data, by using appropriate technical and organisational measures (like pseudonymisation) to ensure compliance with data-protection principles. We will ensure only Personal Data which is necessary for each specific purpose is processed. We will carefully consider the amount of Personal Data we collect, the extent of its processing, the period of its storage and its accessibility. In particular we will control the number of people to whom it is available. Staff should ensure that they adhere to those measures within the Staff Computer Use and Security Policy. For example, in the use of special access-controlled drives for sharing access to personal data, and ensuring encryption methods are applied in the event that the use of attachments cannot be avoided.

9.2 We will have adequate resources and controls in place to ensure and document UK GDPR compliance including:

- Appointing a DPO, who reports directly to the Senior Management Team;
- Integrating data protection into internal documents including this policy, Related Policies and Privacy Notices;
- Regularly training staff on data protection matters, and maintaining a record of that training;

- Regularly resting the privacy measures implemented and conducting periodic reviews and audits to assess compliance; and
- Conducting DPIAs in respect of high-risk Processing before that Processing is undertaken. Instances where a DPIA would be necessary include:

    - The use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
    - Automated Processing including profiling and Automatic Decision Making (ADM);
    - Large scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and
    - Large scale, systematic monitoring of a publicly accessible area, (e.g. CCTV).

9.3 When a DPIA has been identified as necessary, it will include:

- A description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
- An assessment of the necessity and proportionality of the Processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk-mitigation measures in place and demonstration of compliance.

9.4 Staff considering a project which involves Personal Data in a new and/or different way should contact the DPO in the first instance to ascertain if a Data Protection Impact Assessment is required.

9.5 We will keep full and accurate records of all our Data Processing activities, known as our Record of Processing Activity. These records will include:

- The name and contact details of the Controller and DPO;
- Clear descriptions of:

    - The Personal Data types;
    - The Data Subject types;
    - The Processing activities;
    - The Processing purposes;
    - The third-party recipients of the Personal Data;
    - The Personal Data's storage locations;
    - The Personal Data's transfers;
    - The Personal Data's retention period; and
    - The security measures in place.

9.6 Each head of business area will be responsible for the maintenance and regular update of their section of the Record of Processing Activity, supported by the DPO.

10 The Data Controller and the Designated Data Controllers

10.1 The University is a Data Controller under Data Protection Legislation, which means we make the decisions regarding the Processing of the Personal Data that we hold, including in regards to its collection, usage, sharing, storage and deletion. There are designated data controllers who deal with day-to-day matters alongside the DPO.

10.2 We have 3 designated data controllers:

Sharon Bailey	-	Pro-Vice-Chancellor Registry and CFO
Graham Curling	-	Head of Human Resources
Professor Dave Russell	-	Pro-Vice-Chancellor Education

11 Reporting a Personal Data Breach

11.1 We have put in place procedures to deal with any suspected Personal Data Breach and will notify any applicable regulator, including the Information Commissioners Office (ICO), and in certain instances the Data Subject(s), where we are legally required to do so.

11.2 We have put in place procedures to deal with any suspected Personal Data Breach, including making the necessary notifications. If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO (see 4), who will be able to advise on next steps. You should preserve all evidence relating to the potential or suspected Personal Data Breach, and follow and additional instructions issued by the DPO or outlined in the Data Breach Management Guidelines

11.3 Records of Personal Data Breaches must be kept, setting out:

- The facts surrounding the breach;
- Its effects; and
- The remedial action taken.

11.4 These records will be maintained by the DPO and in accordance with the University's Data Breach Management Guidelines.

12 Transfer Limitation

12.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by UK GDPR is not undermined. You make a transfer of Personal Data originating in one country 'across borders' when you transmit, send, view or access that data in or to a different country.

12.2 Occasionally we may need to send Personal Data outside of the UK. Where this is the case, we will ensure that adequate levels of protection are in place to ensure the security of the transfer. Adequacy regulations in the UK currently apply to countries in the EU and EEA and countries covered by existing UK adequacy decisions. Where these regulations do not apply, additional safeguards will be put in place for any necessary restricted transfers of Personal Data.

These include instances where:

- Appropriate safeguards are in place, such as a standard contractual clauses (SCCs) or an international data transfer agreement (IDTA) approved for use in the UK.
- The Data Subject has provided Consent to the proposed transfer after being informed of any potential risks; or
- The transfer is necessary for one of the other reasons set out in the UK GDPR including:
    - The performance of a contract between the University and the Data Subject;
    - Reasons of public interest;
    - To establish, exercise or defend legal claims;

- To protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent; or
- In some limited cases, for our legitimate interest.

12.3 Standard transfer agreements exist between the University and a number of international partners. The DPO should be consulted before any agreement to transfer Personal Data is made.

13 Retention of Data

13.1 We must not keep Personal Data in a form that allows Data Subjects to be identified for longer than needed for the purposes for which we collected it. Those purposes include satisfying any legal, accounting or reporting requirements. Records of Personal Data can be kept for longer than necessary if properly anonymised.

13.2 We will maintain a Record Retention Schedule and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time.

13.3 Staff should take all reasonable steps to destroy or erase from the University's systems all Personal Data that we no longer require in accordance with our Privacy Notices and the University's Record Retention schedule. This includes requiring third parties to delete that data where applicable.

14 Direct Marketing

14.1 The University is subject to certain rules and privacy laws when engaging in direct marketing (for example, when sending marketing emails). For example, a Data Subject's prior consent is generally required for electronic direct marketing.

14.2 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

14.3 A Data Subject's objection to direct marketing must always be promptly honoured. If a Data Subject opts out of marketing at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

15 Sharing Personal Data

15.1 Generally, Personal Data must not be shared with third parties unless certain safeguards and contractual arrangements have been put in place.

15.2 Staff should only share Personal Data with other members of staff, agents, or representatives, if the recipient needs to know the information for the legitimate performance of their duties and the transfer complies with any applicable cross-border transfer restrictions.

15.3 Personal Data can only be shared with third parties, such as service providers, if:

- They need to know the information for the purposes of providing the contracted service;
- Sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

- The third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;
- The transfer complies with any applicable cross-border transfer restrictions; and
- A fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

16 Summary

16.1 Compliance with Data Protection Legislation is the responsibility of all members of the University. Any deliberate breach of this policy may lead to disciplinary action being taken, or even a criminal prosecution.

APPENDIX A

Glossary

Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The Data Protection Legislation, including the UK GPPR, prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of Artificial Intelligence (AI) where they involve the processing of Personal Data.

Confidentiality: only people who have a need to know, and are authorised to use, the Personal Data can access it.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Criminal Convictions Data: Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in accordance with Data Protection Legislation, including the UK GDPR. The University is a Data Controller under Data Protection Legislation.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Legislation: laws that set out how to ensure the proper and fair use of Personal Data, including the UK GDPR as amended, the EU GDPR and the Data Protection Act 2018.

Data Protection Officer (DPO): the person required to be appointed under specific circumstances under Data Protection Legislation.

Integrity: Personal Data is accurate and suitable for the Purpose for which it is processed.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Category Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, Confidentiality, Integrity or Availability or Personal Data or the physical, technical, administrative or organizational safeguards that we or our third-party providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design and Default: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with Data Protection Legislation, including the UK GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the University collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employees, students and prospective students or alumni) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: Policies and procedures relating to, and to be read in conjunction with, this Policy. This includes the Staff Computer Use and Security Policy, Records Management Policy (including Records Retention Schedule), Data Breach Management Guidelines, and specific Data Subject Privacy Notices.

Special Category Personal Data: information revealing, racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

UK GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.