

York St John University Data Protection Policy

Scope:	Staff, contractors and students	Version:	3
Approved by:	Executive Board	Effective date:	September 2024
Responsible department:	Governance and Compliance	Last updated by/date:	Information Governance Adviser, 1 June 2024
Equality analysis undertaken:	Yes	Review date:	September 2025
Associated links:		Policy reference:	

1 Context

This policy is written with due regard to the principles and guidelines laid out in the UK General Data Protection Regulation (UK GDPR); Data Protection Act 2018 (the “data protection legislation”) and other guidance available from relevant professional or regulatory bodies, such as the Information Commissioner. Data protection legislation controls how personal information is used by organisations, businesses or the government.

This policy works in conjunction with the University Data Governance Strategy and the Acceptable Use Policy for IT Facilities and Equipment and applies to records about individuals who can be identified from that data.

2 Purpose

The purpose of this Policy is to ensure that the University, its staff and students, comply with the data protection laws when processing (collecting, recording, storing, using, analysing, combining, disclosing and deleting) personal data.

Personal data is defined as: “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be

identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (*UK GDPR Article 4(1)*)

Personal data that reveals an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health, and individual's sex life or sexual orientation is classed as "special categories of personal data" and merit specific additional protection.

This Policy applies to all personal data processed by the University, regardless of whether that data is held on University equipment or personally owned equipment used inside or outside University premises.

In law the University is a "Controller" required to ensure all personal data it is responsible for is processed in accordance with the data protection legislation. The Controller is also required to ensure anybody acting under their authority i.e., staff, students, contractors, who has access to the University's personal data only processes that data in accordance with the controller's instructions, which are:

Personal data shall be:

- processed lawfully and fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures; and
- the controller shall be responsible for and able to demonstrate compliance with these principles (*UK GDPR Article 5 Paras 1&2*)

3 Responsibilities

University

The University is the Controller and legally responsible for establishing appropriate technical and organisational measures to ensure compliance with data protection legislation.

When acting as a Processor (processing personal data on behalf of another controller under contract), the University is (a) responsible for acting only in accordance with the Controller's documented instructions and (b) ensuring the protection of that personal data through effective organisational and technical measures.

Governance

The University Secretary and Registrar is the Data Protection Officer (DPO) and is responsible for:

- informing and advising the Executive Board and everybody involved in the processing of personal data of their obligations pursuant to the data protection legislation;
- promoting and monitoring compliance with the legislation, including raising awareness and training; producing policy and guidance; providing advice and managing risks.
- ensuring data protection impact assessments are completed appropriately, providing advice and monitoring its performance pursuant to UK GDPR Article 35;
- ensuring compliance with subject access rights and ensuring that data is disclosed in accordance with subject access legislation pursuant to UK GDPR Article 15;
- ensuring data protection breaches are documented, reported, investigated and resolved and when appropriate reported to the Information Commissioner's Office pursuant to UK GDPR Article 33;
- cooperating with the Information Commissioner's Office (*the supervisory authority*); and
- acting as the contact point for the Information Commissioner's Office on issues related to the processing of personal data.

The DPO is also responsible for ensuring the University's Data Protection Notification is registered with the Information Commissioner's Office and for reviewing this Policy in line with current legislation, codes of practice and regulatory standards.

Staff

Access to personal data is only provided to authorised staff who need it to be able to perform their essential contracted duties.

Staff members processing personal data about YSJU students, staff, applicants, alumni or any other identifiable individual must comply with this Policy. This includes any voluntary, short-term or contracted staff.

In particular, staff members must ensure that they:

- comply with the data protection principles when obtaining, using, disclosing or otherwise processing personal data.
- keep all personal data securely in accordance with this Policy and the Acceptable Use Policy for IT Facilities and Equipment and related guidance;
- only disclose personal data to persons authorised to receive it when it is appropriate to do so;

- do not disclose personal data accidentally or otherwise, to any unauthorised person/third party (staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Governance and Compliance office);
- maintain and dispose of personal data in accordance with the University's Records Management Policy and retention schedules;
- direct any queries regarding data protection, including subject access requests and complaints, to the University Secretary's Team;
- report any data protection breaches to the Governance and Compliance office and provide support to ensure the incident is appropriately investigated and resolved;
- seek advice from the Governance and Compliance office about data protection matters when in doubt; and
- ensure students under your supervision are aware of their responsibilities for data protection.

Processors

A "processor" is somebody other than University staff who processes personal data on behalf of the University – usually an external company working under contract.

When a processor is used, the University as Controller retains responsibility and liability for the secure and lawful processing of the personal data being processed. The controller can only appoint a processor:

- who can provide sufficient guarantees about its technical and organisational security measures to protect personal data and meet the requirements of the UK GDPR;
- processes personal data only in accordance with the instructions of the controller set out in a written contract; and
- does not appoint a sub-contractor without the written permission of the controller.

Students

Students are responsible for ensuring compliance with this Policy when processing personal data under the jurisdiction of the University and in particular when conducting research that includes the collection and use of participants' personal data.

4 Lawful Basis for Processing

Any processing of personal data must be done in compliance with the data protection legislation and will only be lawful if one of the conditions in Article 6 – Lawfulness of processing applies; and, where special categories of personal data are used, both a condition in Article 6 and a condition in Article 9 must apply.

Where Article 6 Section 1(f) condition - processing is necessary for the purpose of the legitimate interests (of the University) applies, a Legitimate Interests Assessment (LIA)

must be completed to justify the University's legitimate interests do not override the individual data subject's fundamental rights and freedoms.

5 Rights of the Data Subject

The University respects the fundamental rights and freedoms of data subjects and will uphold their rights by ensuring:

- concise, transparent, intelligible and easily accessible information is provided to explain the reasons why the University collects and uses personal data and the lawful basis;
- subject access requests are responded to fully in accordance with UK GDPR Article 15 (subject to verification of identity and right to access);
- rights concerning rectification, erasure, restrictions, portability and erasure of personal data are upheld (unless the University cannot comply for legal reasons and is required to apply an exemption)
- the individual data subject's legitimate right to object to the processing of their personal data for certain purposes is respected;
- consent is obtained when it is required to provide the lawful basis for processing personal data; and
- personal data is protected by technical and organisational controls at all times.

6 Information Security

Technical and organisational measures shall be implemented to ensure personal data is protected against risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed which may lead to physical, material or non-material damage.

The University's Acceptable Use Policy for IT Facilities and Equipment and guidelines should be followed to ensure the protection of:

- **Confidentiality** - ensuring that personal data is only accessible to authorised users;
- **Integrity** - safeguarding the accuracy and completeness of personal data; and
- **Availability** - ensuring that authorised users have access to information and systems when and where required.

Staff, students, volunteers, contractors, and any other individuals who are required to handle University data should ensure that they do so safely and securely when accessing data off campus and/or via shared spaces.

Staff Working Remotely

10.1 Cloud Storage

Individuals should only access data from and save data within the University's OneDrive, via the Virtual Desktop Infrastructure (VDI), or using recommended software and applications. Data should not be stored on the hard drive of personal computers, smartphones, tablets or other portable devices. It may be necessary to store or capture data using a USB memory stick, smartphone, or recording device and the individual should ensure that these devices are encrypted with a password and not left unattended. All removable media and portable devices should be kept in locked storage or a secure area when not in use.

10.2 Security Software

Individuals should ensure that their personal computer is equipped with antivirus software and that all software and operating system updates are installed. Due to capabilities of recent editions of operating systems such as Microsoft Windows and MacOS, it may not be necessary to install third-party antivirus software.

10.3 Home Wi-Fi

Individuals who use their home wireless network for work should ensure that it is secured with a password, that the password is only made available to trusted parties and that the password has been changed from the default one supplied. If a home wireless network is left unsecured, information including logins, passwords, messages, and other sensitive data can be more easily intercepted.

10.4 Public Wi-Fi

If an individual is using a public wireless network, they cannot guarantee that their connection is safe and secure. If sensitive data is being accessed in these spaces, it is recommended that Virtual Personal Network (VPN) software is installed and activated. If an individual cannot guarantee a safe connection, they should not access sensitive data until a secure connection can be made.


10.5 Clear Desks

When working within a home environment, individuals should ensure that they have a clear and tidy space to work and that any sensitive data isn't exposed or left behind. If the individual works with hardcopy data, lockable storage is essential for when the information isn't in use. If the individual accesses sensitive data on screen, they should be aware of their surroundings and ensure that information is minimised or closed when other individuals are present. If removable media is used, such as USB memory sticks or recording devices, they should be encrypted and always removed and securely stored when the individual vacates their workspace.

10.6 Spatial Awareness and Screen Security

When working in a shared space, it is essential to be aware of your surroundings. Individuals should try to position themselves in an area where other individuals cannot clearly view the computer screen or see information in hardcopy format. When typing passwords, ensure that the keys and screen cannot be easily seen by other individuals, and ensure that data is minimised or closed when not in use. Do not leave devices or hardcopy data unattended and always check and double check that you have all your belongings before you vacate the area.

If you are going to be away from your desk, ensure that you lock your computer when you are not using it, even if you only intend to be away from your desk for a few minutes.

Screens can easily be locked when not in use by using the Windows key  and 'L' for Windows computers, or Control/Shift/Power for Macs.

10.7 Device Encryption

All digital devices should be secured with a password. This includes, but isn't confined to, desktop PCs, laptops, USB memory sticks, smartphones, and recording devices. The password should remain confidential and changed regularly. Where possible these devices should be encrypted. Most modern devices have an encryption option or come encrypted by default. Device encryption is never more important than when working in a shared space as, if they are left behind, other individuals will require a password to access data.

10.8 Data Disposal

Hardcopy data such as paperwork and notes should be shredded and securely disposed of when no longer required. It's essential that individuals are aware of their departmental retention schedule and that data disposal is processed accordingly. Digital data should be securely deleted when it is no longer required. Individuals should ensure that the data is deleted from all access points, including recycle bins. Further information concerning the secure disposal of confidential and sensitive data can be found in the University's Records Management Policy.

Staff Working on University Premises

10.9 Clear Desks

When working on University premises, individuals should ensure that they have a clear and tidy space to work and that any sensitive data isn't exposed or left behind. If the individual works with hardcopy data, lockable storage is essential for when the information isn't in use. Lockable storage should, however, only be used for records which cannot be converted to digital format and stored securely on the University's systems. Any handwritten data should only be stored in lockable storage temporarily until it has been transcribed and stored digitally or is no longer required. All handwritten data, including meeting notes and forms, should be converted into a digital record as soon as possible and the original securely destroyed. If the individual accesses sensitive data on screen, they should be aware of their surroundings and ensure that information is minimised or closed when other individuals are present. If removable media is used, such as USB memory sticks or recording devices, they need to be secured with a password and should be encrypted where possible and always removed and securely stored when the individual vacates their workspace.

10.11 Spatial Awareness and Screen Security

When working in a shared space, it is essential to be aware of your surroundings. When working with sensitive or confidential information, individuals should try to position

themselves in an area where other individuals cannot clearly view the computer screen or see information in hardcopy format. When typing passwords, ensure that the keys and screen cannot be easily seen by other individuals, and ensure that data is minimised or closed when not in use. Do not leave devices or hardcopy data unattended and always check and double check that you have all your belongings before you vacate the area. If you don't have access to lockable storage, alert your manager as soon as possible.

10.12 Whiteboards and Sticky Notes

If you have recorded any sensitive data on whiteboards, pinboards, or on sticky notes in your immediate area, ensure that everything is wiped, removed or shredded before you vacate the area. Do not use standard bins to discard of sticky notes which contain sensitive data; these should be shredded and disposed of via confidential waste bins.

7 Personal Data Security Incidents

A personal data security incident is any incident that involves a failure of the University's technical and organisational measures resulting in any unauthorised or unlawful processing, accidental loss, destruction of or damage to personal data.

The GDPR introduces a new duty on all organisations to report certain types of personal data incidents to the Information Commissioner's Office within 72 hours of becoming aware of the incident. In certain circumstances individuals whose personal data has been compromised by the incident must also be notified. A risk assessment should be made by the Governance and Compliance team in liaison with the DPO when considering external communication or elevation of the incident.

The Governance and Compliance office must be informed of a data security incident as soon as it becomes known and their advice should be followed without delay. The procedure is outlined on the Staff Intranet.

8 Privacy by Design

Organisations should carry out a Data Protection Impact Assessment (DPIA) prior to embarking on a project that has an impact on the way personal data is processed e.g. the implementation of a new IT system for collecting, storing and accessing personal data; a new data sharing initiative etc. A DPIA enables the organisation to identify and mitigate the associated privacy risks and ensure data protection compliance is built into the design, including being able to demonstrate compliance with legal obligations.

The University's Data Protection Impact Assessment Procedure should be followed when:

- developing a new IT system for storing and accessing personal data;
- negotiating a new data sharing initiative where two or more organisations seek to pool

or link sets of personal data;

- designing a proposal to identify people in a particular group or demographic and initiate a course of action e.g. profiling or research;
- planning to use existing data for a new and unexpected or more intrusive purpose;
- introducing new policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

The University's DPO is responsible for providing advice, ensuring the process is completed appropriately and monitoring its performance pursuant to UK GDPR Article 35.

9 Information Asset Register

The Data Controller should maintain a record of processing activities under its responsibility, and specifies what information that record should contain.

YSJU has an Information Asset Register for this purpose. It is managed by the Governance and Compliance team.

10 Guidance

The Information Commissioner's [Guide to the GDPR](#) explains the provisions of the GDPR to help organisations comply with its requirements

11 Review

The University Secretary, as the DPO, is responsible for reviewing this Policy in line with current legislation, codes of practice and regulatory standard. The Executive Board is responsible for approval of the Policy.

The Policy will be reviewed on an annual cycle, or sooner in response to relevant changes in legislation.