Futureworks

Version Control Statement

ID Number:	FW002	**Document Name:**	Data_Security_Policy_V2.0.0		
Approving Committee:	Operations Team				
Last Review:	Nov-23		**Next Review:**	Jun-25 to Aug-25	
Owner:	Head of Registry Services & Business Intelligence		**Review Lead:**	Head of Registry Services & Business Intelligence	
Amendments Since Approval:	**Detail of Revision:**			**Date of Revision:**	**Revision Approved by:**
	Section headers added			July 2023	Executive Team
	More in depth information regarding access, transmission of data and storage given.			July 2023	Executive Team
	Executive Committee replaced with Operations Team as approving committee			10/09/24	Operations Team

If this document is required in an alternative format, please contact Futureworks on 0161 214 4600 or via email: info@futureworks.ac.uk

Futureworks Data Security Policy

1.0 Purpose

The purpose of this Data Security Policy is to ensure the protection of data processed, stored, transmitted, and managed by Futureworks, to preserve the confidentiality, integrity, and availability of this data, and to comply with all relevant legislation and contractual requirements.

2.0 Scope

This policy applies to all faculty, staff, students, contractors, and any other parties who have access to or manage Futureworks' data and related systems, regardless of location.

3.0 Policy

3.1 Data Classification

All data within the control of Futureworks will be classified into one of three categories based on its sensitivity:

- Public Data: Information that may be disclosed to any person, without any restrictions.
- Internal Data: Information that is not generally available to the public, but not highly sensitive.
- Confidential Data: Highly sensitive information, disclosure of which would cause significant damage.

3.2 Access Control

Access to data shall be restricted based on the principle of least privilege, which ensures individuals, software processes, and systems have access only to the data and resources that are necessary for their legitimate purposes. Access controls should align with defined roles and responsibilities.

3.2.1 User Access Management

User access to systems and data should be granted following a formal user registration and provisioning process. This process should include a review and approval by the appropriate authority.

3.2.2 User Identification and Authentication

All users are required to authenticate themselves using a unique identifier (username) and password, or other forms of identification and authentication as applicable (e.g., two-factor authentication), before they can access Futureworks systems and data.

3.2.3 Role-Based Access Control (RBAC)

Access to data will be based on the role of the user within Futureworks. Roles are defined based on the authority, responsibilities, and job functions. Individuals are assigned roles, and through those roles, access permissions are granted.

3.2.4 Access to Confidential Data

Access to confidential data is limited to those who require the data to perform their job function. All access to confidential data must be logged, and logs should be regularly reviewed for any unusual or unauthorised activities.

3.2.5 User Access Review

The access rights of all employees and external parties should be reviewed at regular intervals, or at a minimum annually. The review should ensure that access rights remain appropriate and necessary.

3.2.6 Revocation of Access

Upon termination of an employee or contractor, all access to systems and data must be promptly revoked. The IT department must be notified in advance of the termination or completion. Students may be granted extended access to certain accounts after leaving their programme of study if a graduate license is appropriate and available.

3.3 Data Transmission

Data transmission refers to any mechanism by which data is transferred from one location to another. This includes but is not limited to email, cloud storage, file transfer, and other forms of electronic communication. It is essential that data transmission is secure to prevent unauthorized interception, alteration, or destruction.

3.3.1 Secure Transfer

All data transmission over networks must use secure, encrypted communication channels, such as Secure Socket Layer (SSL), Transport Layer Security (TLS), or Internet Protocol Security (IPSec) protocols.

3.3.2 Email Communication

Confidential data must not be sent over email unless the attached data is securely sent using password protection. In general, users should avoid sending sensitive information through email, particularly to email addresses outside Futureworks' domain. The preferred method for sharing data within Futureworks' environment would be through Teams or shared 365 folders. For external sharing, please contact the Head of Registry Services for advice.

3.3.3 Remote Access

Staff access to Futureworks' internal networks from remote locations must be secured using Virtual Private Networks (VPN) or other secure remote access methods. Two-factor authentication (2FA) should be used for remote access where possible.

3.3.4 Data Transfer with External Parties

Any transfer of data to external parties must be conducted securely and in accordance with data sharing agreements, and legal and regulatory requirements. All external transfers should be logged and subject to routine audits.

3.3.5 Wireless Transmissions

Wireless networks are inherently insecure due to their nature. Therefore, when transmitting confidential data over wireless networks, it must be encrypted, and the network must use robust security protocols.

3.3.6 Mobile Devices and BYOD

Mobile devices (smartphones, tablets, laptops, etc.) pose a significant risk to data security during data transmission. Employees using mobile devices for work should follow Futureworks's Mobile Device Policy. Bring Your Own Device (BYOD) must also follow appropriate security protocols including encryption, remote wipe capability, and automatic locking.

3.3.7 Cloud Services

If cloud services are used for data storage or transfer, they must be approved by the Futureworks IT department, and a contract must be in place that guarantees the security and privacy of the data.

3.4 Data Storage and Disposal

Data storage involves the use of physical or virtual resources to retain digital information, while disposal refers to the final disposition or deletion of data. All data must be securely stored and disposed of to prevent unauthorized access, alteration, or deletion.

3.4.1 Secure Data Storage

All data, particularly confidential data, should be securely stored using appropriate security controls. This includes maintaining physical security for hardware storage devices and implementing logical controls for data stored in electronic format.

3.4.2 Data Encryption

Confidential data, both at rest and in transit, should be encrypted using a secure and approved encryption algorithm. This includes data stored on hard drives, USBs, laptops, servers, and cloud storage.

3.4.3 Physical Security

Physical access to data storage facilities, including server rooms and data centres, should be strictly controlled. Only authorized personnel should have access to these areas.

3.4.4 Cloud Storage

Cloud storage solutions, if used, must provide robust security measures including data encryption, access control, and a clear data deletion process. Cloud storage providers should be chosen carefully, and a proper due diligence process should be followed.

3.4.5 Data Backup

Futureworks should have a robust data backup and recovery plan in place. Backups should be encrypted and stored in a secure off-site location. The backup and recovery processes should be regularly tested.

3.4.6 Data Disposal

Data that is no longer needed should be disposed of in a secure and permanent manner. This includes deleting electronic data and physically destroying hardware storage devices. Disposal methods should prevent the reconstruction or retrieval of the data.

3.4.7 Secure Deletion of Electronic Data

Before the disposal or repurposing of any storage media (hard drives, SSDs, flash drives, etc.), all data should be securely wiped using methods that meet recognized industry standards. Hardware containing drives should be sent to Facilities who will arrange to use the services of a company that provides a secure data destruction certificate.

3.4.8 Disposal of Physical Records

Physical records containing confidential data should be securely destroyed when they are no longer needed. This can be achieved through methods such as cross-cut shredding, burning, or contracting with a trusted third-party document destruction company.

3.4.9 Disposal Record

A disposal record should be maintained documenting what data was disposed of, the reason for disposal, the method of disposal, and the date of disposal. This record can help demonstrate compliance with data retention and disposal laws and regulations.

3.5 Incident Response

In the event of a security breach, the Data Breach Notification policy should be followed, and the Data Protection Officer informed immediately.

3.6 Training

Futureworks will provide regular training on this policy and other data security issues to all relevant parties.

4.0 Roles and Responsibilities

The Futureworks' Data Protection Officer is responsible for the oversight of this policy. All members of the Futureworks community have a responsibility to protect the data they use.

5.0 Review and Updates

This policy will be reviewed annually, or as required by changes in legislation or technology.

6.0 Compliance

Violation of this policy may result in disciplinary action, up to and including termination for employees or expulsion for students, and legal action where applicable.

7.0 Definitions

- Data: Any information that is used by or belongs to Futureworks or that Futureworks is responsible for.

- Confidential Data: Data that Futureworks is legally, contractually, or ethically obliged to protect.
- Encryption: The process of encoding data to prevent unauthorized access.