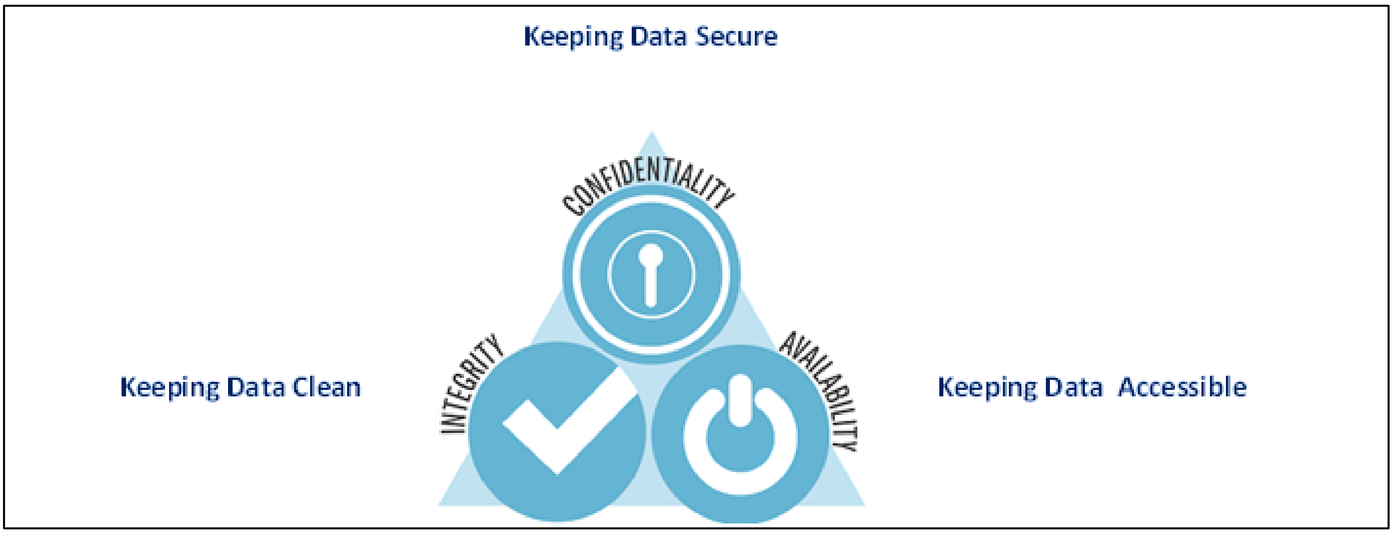
Sheffield Hallam University

Data Protection for Researchers:
Data Security and Storage

GDPR requires organisations to implement appropriate technical and organisational measures to keep data secure. i.e. appropriate to the risks, depending on the type of data and processing.

Risks:

The risks can be expressed as the loss of Confidentiality, Integrity, and Availability of data, processing and systems (CIA).



Keeping Data Secure

Keeping Data Clean

Keeping Data Accessible

- Security and protection of data is a critical consideration in planning its storage. Without assessing the risks fully the potential of loss or exposure of the data through cyber security threats or vulnerabilities.
- Cyber security is a growing risk through vulnerabilities in technology enabling attackers to take advantage of weaknesses in practice or configuration. The worldwide trend is that cyber security attacks are increasing and education and research organisations are amongst the most frequently attacked.
- Human error in relation to emails and transferring data continue to be one of the most frequent types of data breaches.
- Managing access to files and updating the access permissions when staff and requirements change are also key to good data security.

Appropriate measures are not defined or specified in the legislation and need to be assessed according to the specific processing and data but may include:

- robust policies and procedures;
- clearly defined roles and responsibilities for the management of data;
- technology – encryption, firewalls, anti-virus, anti-hacking technology and measures, password protection of files;
- locking away paper files, laptops, memory sticks etc.;
- restricting access to offices, databases, filing systems, folders within shared drives and managing permissions;
- ensuring data is backed up and protected from loss or damage
- disposing of data securely - shredding, confidential waste, secure disposal of IT equipment etc.;
- care when mobile working;
- anonymising and pseudonymising data where possible and appropriate;
- staff induction, training, awareness, self-regulation.

Encryption of data is a key element of data security. All portable/mobile devices (laptops, tablets, smartphones, portable hard drives, USB sticks, dictaphones etc.) MUST be encrypted. Emails should be encrypted where they contain special category personal data or large volumes of personal data. The University Encryption Policy outlines the requirements for data leaving the University to do so securely.

Conducting a **Data Protection Impact Assessment (DPIA)** will help you to consider the risks and appropriate measures that you can then include in a data management plan.

Data Storage

Where to save and store personal data:

- **F Drive, SharePoint, Onedrive, N Drive,** for files containing personal data – must have appropriate access/permissions management in place for N drive folders and sharepoint.
- **J drive** for research data containing personal data/sensitive data or where there are contractual obligations that require greater levels of security and audit trail. Requests for J drive can be logged via https://itservicedesk.shu.ac.uk/. Large file/datasets can be accommodated but please flag this early so DTS staff can ensure you have sufficient storage allocated.
- **Q drive research files** ideal for anonymised data and pseudonymised personal data (key stored separately in different location), and lower risk personal data ok. Avoid very sensitive data on Q and where there are contractual requirements for audit trails of usage/access.

Avoid saving files to:

- **A local device or drive**, i.e. a local drive on a personal or SHU owned PC or laptop (e.g. C or D) - UNLESS the files are duplicates of, and synchronising with, the original/master files in a cloud based location, or a network drive.
- **USB sticks or USB hard drives** - UNLESS they are duplicates of originals needed as a backup or for access in a location which has no other means of accessing the originals (device must be encrypted for personal data).
- ***Personal/Private* cloud storage services** (e.g. OneDrive / Google Drive / Dropbox etc). University cloud services and storage are assessed and configured to ensure data can be stored complying with security and regulatory requirements. Although many of these have personal services that are often available for free they are not covered by the same terms and conditions and are not compliant with University policies. Data in personal services is also at risk of being lost to the University if the owner leaves.
- The use of **other non-SHU software** for work purposes is also not advised as the security and compliance measures may not be sufficient and there will be no obligation from the provider to continue the service or to return data to users. Please check with DTS if you wish to use different software.
- **Any device which can be accessed be accessed by other members of your household using YOUR account.**

Use of these to store data will expose it to potential loss, either leaving you without the data or exposing it to unauthorised people. Storage provided by the University is secure, resilient against failure and backed up to ensure that data is safely stored. There is no need for you to be backing up University data stores independently.

Digital Skills Hub Guidance on storing and sharing data (Covers other options for personal and non-personal data): https://sheffieldhallam.sharepoint.com/sites/4042/SitePages/Where-do-I-save-and-share-my-work-.aspx

Sharing personal data with external collaborators

Do use for sharing research data containing personal data:

- ZendTo – using Microsoft encryption or 7Zip

- SHU encrypted email How to Send Encrypted Emails (sharepoint.com)
- Sharepoint/Teams guest access Guest Access in Teams (sharepoint.com) and Guest Access in Teams (sharepoint.com)
- Access to Q drive folders

External collaborative partners may suggest other data sharing methods. If you are not sure whether these are secure or compliant, please contact the IT Helpdesk and/or IG Team.

Where access to University folders is given, good governance and data management needs to be in place to ensure that access continues to be appropriate and necessary. In particular consider risks around staff leavers and access at different stages of the project, including the end of the project.

Don't use for sharing research data containing personal data:

- Unencrypted email
- Private/non-University cloud services or communications channels
- Unencrypted USB sticks

The use of **Google Drive** involves data being transferred to the USA. This is generally not advised for personal data, as it is difficult to make this fully compliant. It should particularly not be used for sensitive/special category personal data, or for contracts where the data is required to stay in the UK or EU.

Data Security Incidents and Breaches

The University takes its data protection responsibilities very seriously and puts in place guidance, training, procedures and policies to keep personal data secure. However, given the scale and complexity of the organisation and the range and volume of information processed by the University, it remains possible that some data incidents will occur. When they do, it is essential to minimise the damage caused and to learn from the incident to prevent repetition.

What is a data security breach/incident?

A security breach is:

- an event or series of events leading to the unintentional or unauthorised disclosure of information which compromises the security, confidentiality or integrity of data. This would generally be seen as the loss or theft of data and could apply to paper documents or electronic data. However, unauthorised access to data could also be a security breach, e.g. someone seeing data on a screen or desk without authorisation, permissions/access to electronic data being set up incorrectly.
- the intentional, unauthorised disclosure of information, except for disclosures which fall into the category of whistleblowing. This would include, for instance, unauthorised disclosure of data for personal or financial gain.

Ask yourself:

- Has personal data been lost or stolen?
- Has a device on which data is stored been lost or stolen?
- Has someone accessed personal data that they shouldn't have accessed?
- Have you found personal data that you don't think you should be able to access?
- Have you shared data with someone that wasn't entitled to have it?
- Has your IT account been compromised? Is there any unusual activity on your account?
- Have you responded to a phishing email or provided your login details outside the University?
- Do you think personal data has been hacked?
- Have data or equipment been disposed of in an unsecure way?

A data security incident is categorized in one of three ways:

- **Data Security Breach-** an event or series of events that could threaten the confidentiality and/or integrity of data, e.g. loss, theft, compromise of systems, distribution to third parties in error.
- **Near Miss-** incidents which did not result in the loss or theft of personal data but had the potential to do so and where there is the possibility of a future breach, either because there is a weakness in a policy or process or a vulnerability in a system. They may point to a possible weakness which could result in a future loss or corruption of data.
- **No Incident-** After an investigation a decision is made that no breach occurred and there is no potential for a future breach because of a weakness.

Required Action and Staff Responsibilities

- **Staff must report data security breaches IMMEDIATELY to the IT Service Desk X3333.** The Out of Hours service will report any incidents to the University and will escalate serious incidents to IT managers and the DPO.

- The University has a **Data Breach Management Procedure** and staff are expected to provide information to the IG Team to assist with investigations and may be required to take actions to contain the breach, to recover data, to minimise the impact on data subjects, and to notify other parties of the breach.

- It may not be clear at the outset whether an incident has actually resulted in a data breach or how serious the incident is. We ask staff to report all incidents in order that they can be investigated and assessed and so that we can monitor trends and consider what additional measures and guidance may be appropriate.

- Staff must also report 'near misses' or 'close calls' - this may assist the University to identify procedures that could be improved or risks that need further controls in place.

- **Where the research is governed by a legal contract with a funding body or collaborative partners**, there may be a contractual requirement to inform the funder or the partners within a specified time period. Please seek advice from the IG Team if this applies (DPO@shu.ac.uk). If the University is a data processor for another data controller, we are legally obliged to inform the controller "without undue delay".

- **If you are sent data in error by a colleague:**
  - If you are the only recipient, delete the email from your inbox and your deleted items folder and inform the sender.
  - If you are one of many recipients, you should report this immediately to the IT Service Desk. It may be possible for the email to be deleted from the email system to avoid everyone opening the email.

- **If you are sent data in error by another organisation**, alert the sender of the email and follow their instructions to delete the data. If you use this data for any other purpose you may commit an offence. You can also seek advice from the University's IG Team.

Common security breach types:

- Email errors – wrong recipients, not using BCC, errors with similar names or names appearing in auto-fill, re-using emails instead of using templates, sending to large group or mailing list by mistake. See additional guidance.

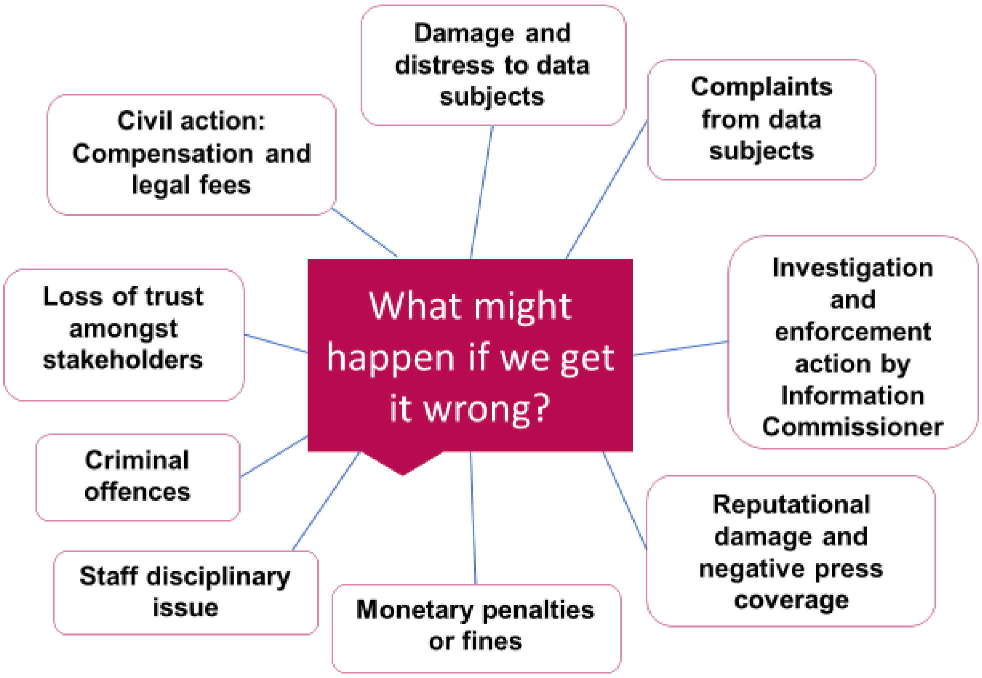
- Lost or stolen laptops, lost or forgotten papers. See guidance on mobile working.

- Incorrect access settings on documents – sharing/publishing too widely.

- Phishing attacks. See CyberAware course.

Common theme: human error – rushing to complete tasks, too many windows open at the same time, staff working when they are ill, not checking emails or documents before sending.

Potential consequences of a breach:


What might happen if we get it wrong?
Damage and distress to data subjects
Complaints from data subjects
Civil action: Compensation and legal fees
Loss of trust amongst stakeholders
Investigation and enforcement action by Information Commissioner
Criminal offences
Staff disciplinary issue
Monetary penalties or fines
Reputational damage and negative press coverage

Additional Guidance:

- **GDPR online module**: https://sheffieldhallam.sharepoint.com/sites/3037/SitePages/Information-Governance-training.aspx
- **Safe use of email** guidance: Governance, Legal and Sector Regulation - Safe Email advice.pdf - All Documents (sharepoint.com)
- **Mobile working** guidance: Governance, Legal and Sector Regulation - Mobile working data security.pdf - All Documents (sharepoint.com)
- **CyberAware course**: Protecting the University from cyber threats (sharepoint.com)
- **Data Breach Management Procedure:** https://sheffieldhallam.sharepoint.com/sites/3037/SitePages/Data-Incident-Breaches.aspx
- **Encrypted emails:** How to Send Encrypted Emails (sharepoint.com)
- **Data Encryption Policy and other DTS IT Policies** IT Policies and Regulations

Further Information and Support: Information Governance Team

Sharepoint: https://sheffieldhallam.sharepoint.com/sites/3037/SitePages/Information%20Governance.aspx

Email: DPO@shu.ac.uk