The University Of Sheffield.

University Secretary's Office.

The University of Sheffield

Data Protection Policy

Version 1.3 – Updated 16 January 2024

Owner: Luke Thompson, Head of Data Protection & Legal Services

1 Introduction

1.1 Purpose of the Policy

The University of Sheffield's Data Protection Policy has been produced to ensure compliance with the General Data Protection Regulation (GDPR) and associated legislation, such as the Data Protection Act 2018. This policy incorporates guidance from the Information Commissioner's Office (ICO) and other relevant organisations.

The Policy provides a framework for compliance and will be supported by a series of additional policies and guidance documents focussing on specific areas of data compliance within the University. The guidance documents will be used to provide advice and keep staff up-to-date with good practice.

1.2 Policy Objectives

The Policy's objectives are:

- to ensure staff are aware of the statutory duties the GDPR and other relevant data protection legislation places on the University;
- to ensure staff are aware of their legal obligations and responsibilities under the GDPR and other relevant data protection legislation;
- to provide clarity to staff on key aspects of data protection legislation;
- to ensure staff are aware compliance with this policy and associated legislation is a requirement and any member of staff who fails to comply may be subject to disciplinary action.

1.3 Help with this Policy

Guidance and clarification about the interpretation or any other aspect of this policy is available from the University Secretary's Office they can be contacted at dataprotection@sheffield.ac.uk

2 Scope

2.1 Who is covered by this Policy?

This policy applies to all staff at the University. This includes temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, the University.

This policy also covers any staff or students who may be involved in research or other activity that requires them to process or have access to personal data (see section 2.2), for instance as part of a research project or as part of professional practice activities. In such cases, it is the responsibility of the relevant department to ensure that research data is processed in accordance with relevant data protection legislation (including the GDPR) and that students and staff are advised of their responsibilities. Research activity should be referred to the Research Ethics Committee or other appropriate University authority.

2.2 What Data is covered by the Policy?

This policy is concerned with personal data (including Special Category data) as defined by the GDPR. Personal data is any information relating to a living individual who can be directly or indirectly identified, by reference to an identifier, such as a name, an identification number, location data, or an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Examples of categories of personal data include:

- Name
- Date of birth
- Address
- National insurance number
- Passport number
- Payroll number
- Student ID
- Comments made about an individual in email
- IP Addresses

Special Category (formerly known as sensitive personal) data is a subset of personal data and means personal data consisting of information relating to;

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- Genetic data (used for identifying an individual),
- Biometric data (used for identifying an individual),
- Data concerning an individual's health,
- An individual's sex life or sexual orientation.

Any processing of criminal offence data should be handled similarly to Special Category data, by determining the legal basis of processing in accordance with Article 6 of the Data Protection Act, with the condition of also ensuring compliance with Article 10. Collecting, or further processing criminal offence data, should be approved by the University Secretary's Office they can be contacted at dataprotection@sheffield.ac.uk

3 The Data Protection Legislation

Data protection legislation (GDPR and the Data Protection Act 2018) provides a framework for organisations (controllers) which ensures personal data is handled properly, as well as providing legal rights to individuals (data subjects). The legislation works in two ways: firstly, it states anyone who processes personal data must comply with the data protection principles, as defined by the relevant data protection legislation; secondly, it provides individuals with important rights, including the right to find out what personal data is held, about them,in both digital and paper records.

3.1 The Data Protection Principles

Data protection legislation requires the University (as a controller), its staff and others who process or use any personal data to comply with the data protection principles. The principles are listed below:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Full wording of the data protection principles is provided at Annex 1.

3.2 Rights of Individuals

The GDPR, provides various rights to individuals, these are listed below;

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (right to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object
- Rights relating to automated decision making including profiling

If any member of the University receives a request relating to any of the above rights it must be sent immediately to the University Secretary's Office who will process it.

The most commonly exercised individual right is that of the right of access. The right of access allows an individual to know what information the University holds and processes about them. This is known as a subject access request, which also provides for individuals, to be given a copy of the information, as well as supplementary information, such as where and with whom the information may have been shared. The right of access, like many of the individual rights, is not an absolute right and disclosure of the requested information is subject to exemptions.

Unless the information requested is provided as part of the normal course of business, the individual who is the subject of the data (the data subject) should be directed to the University Secretary's Office they can be contacted at dataprotection@sheffield.ac.uk for advice on how to make a Subject Access Request (SAR). The University must respond to these requests within one month of their receipt.

3.3 Registration and Notification

As a data controller, the University is required to register with the Information Commissioner's Office (ICO) and submit an annual notification listing the purposes under which it processes personal information. The University must also notify the ICO within 28 days should any entry become inaccurate or incomplete. The ICO publishes a register of controllers on its website which is available to the public for inspection. The University's notification can be found on the ICO's website by entering its registration number: Z681065X

It is an offence for the University to process personal data that falls outside of the purposes declared in its notification, unless these are exempt. Staff who work with personal data should be familiar with the University's notification and inform the University Secretary's Office if they intend to implement changes that may require the University's notification to be amended.

3.4 The Information Commissioner's Office

The ICO is the UK's independent authority (Supervisory Authority) established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO enforces and oversees the relevant data protection legislation as well as the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations. The ICO has the power to take regulatory actions to enforce compliance with the data protection legislation which include enforcement notices, audit, monetary penalties (up to a maximum of 4% of the controllers gross annual turnover or €20,000,000 whichever is higher).

The ICO also receives and responds to complaints from individuals and organisations who feel they are being denied access to personal data they are entitled to, or feel their information has not been handled according to the data protection principles or legislation. Communication with the ICO is conducted by the University Secretary's Office. If you are conducted by them please contact the University Secretary's Office.

Further information about the ICO can be found on its website at http://www.ico.org.uk

4 Responsibilities

University staff who process personal data as part of their duties must ensure they are complying with the Data Protection Principles described in section 3.1, and more generally in compliance with relevant data protection legislation. "Processing" data is a collective term for any action taken relating to personal data and includes obtaining, recording, storing, using, sharing, disclosing, transferring, or destroying data.

4.1 Obtaining Personal Data

Only personal data necessary for a specific University-related business reason should be obtained, and it should be collected in a secure manner.

A privacy notice (also known as a fair processing notice) must be actively communicated to an individual at the point their personal data is collected, and subsequently if requested by individuals. Ideally the privacy notice should be provided in the same medium, in which the data was collected. A privacy notice must as a minimum include the following:

- The name and contact details of the Controller
- Contact details of the University's Data Protection Officer(s)
- The purposes of the processing
- The legal basis of this processing
- Details regarding any processing based on legitimate interest
- Categories of personal data being processed
- The recipients or categories of recipients of the personal data
- Details regarding any transfers of personal data to a third country, or international organisations
- Retention periods for the personal data
- Information regarding individual rights
- The right to withdraw consent (if this is the basis of the processing)
- How to make a complaint, and how to do so
- Details of any statutory or contractual processing
- The existence of any automated decision making, including profiling
- Details of any examples where the controller is likely to process the personal data for a different purpose than it was originally collected

The University Secretary's Office drafts Privacy Notices. They can be found here

If you feel the Privacy Notices need updating please contact University Secretary's Office (dataprotection@sheffield.ac.uk)

In some cases individuals will have a choice as to whether or not to provide their personal data, or the use that can be made of it. In these cases clear consent must be obtained. All consent mechanisms must be compliant with the threshold stipulated by the GDPR. 'Opt-out' consent is no longer valid.

4.2 New Processing

When new projects and initiatives are being developed within the University that could have implications on individuals' privacy, the University Secretary's Office. Where the project has a technical element or relies on software IT Services should also be contacted to identify and assess any privacy concerns. A Data Protection Impact Assessment (DPIA) must be completed; when a new purpose or project will include the processing of personal data, when there is any high risk (including large scale) processing, and when new technology is introduced. The DPIA screening questions at Annex 3 should be answered. Answering yes to any of those questions will mean a complete DPIA is required, to undertake this please contact dataprotection@sheffield.ac.uk

Staff must comply with the concept of Data Protection by Design and Default. This is a mandatory concept enforced by the GDPR, from the beginning and throughout the lifecycle of personal data.

Data Protection by Design and Default requires controllers to implement appropriate technical and organisational measures:

• Which are designed to implement the data protection principles;
• Ensuring that, by default, only the minimal amount of personal data are processed for each of the processing purposes. (This is when privacy enhancing techniques, such as anonymisation and pseudonymisation, should be considered)

4.3 Recording Personal Data

Staff must ensure mechanisms are in place for keeping personal data accurate and up-to-date and for the purpose for which it is held.

Personal data should be retained in accordance with any retention period specified in the relevant privacy notice, and in accordance with the University's Records Retention Schedule.

Staff should be aware that any material they produce, which refers to an individual (or individuals) may be accessed by the individual, regardless of; the informality of the information, how or where it is held, including data held in email accounts. This includes any opinion of or about the individual. Staff should be aware of this when documents/records are created, including emails.

4.4 Emails

The University provide their staff with email accounts. These email accounts and the information contained within are a corporate assets and as such the data is processed and controlled by the University. The email accounts of staff may be accessed for a number of reasons including but not limited to, processing a right to access request, mitigating a data breach and to assist with any misconduct investigation(s). Staff should not be using private email addresses to undertake University work, any email addresses that have University data in may be accessed by the University.

4.5 Processes

Staff whose work involves processing personal data, whether in electronic or paper form, must take personal responsibility for its secure storage.

Access to personal data, in electronic or paper form, should be restricted to staff who need to access the information in the course of their duties.

Personal data in paper form must be kept in a lockable filing cabinet, cupboard, drawer or behind a locked door.

Documents containing personal data should only be printed when there is a business need to do so. Documents should only be 'pull' printed to a shared device, and removed immediately once printed by the member of staff who printed them.

Personal data in electronic form should be stored within the University Data Centre (which is regularly backed up) and should not be kept on local hard drives. As a minimum, user accounts should be password protected in line with the University's IT Authentication Policy and consideration should be given to the use of additional folder, file or database level password protection, access restrictions and/or encryption. Staff can contact the University's IT Services for advice on this.

Staff who intend to store personal data on a portable storage device, such as; a laptop, tablet, memory stick, hard drive, disk or mobile phone, must seek the authorisation of their line manager. The personal data on the portable storage device must be encrypted and the device must be kept in a lockable filing cabinet, cupboard or drawer. (Please refer to the University's Acceptable Use Policy framework here)

Staff must not keep special category data (see section 2.2) on portable storage devices unless they have received authorisation from both their line manager and the University Secretary's Office.

Personal data should never be stored at staff members' homes, whether in paper or electronic form. In instances where off-site processing is necessary, staff must obtain authorisation from their line manager. If the processing includes special category (sensitive) data (see section 2.2) the authorisation of both their line manager and the University Secretary's Office is required.

If personal data are processed off-site electronically, this must be done so using University approved equipment and/or systems (including remote access mechanisms)

When processing personal data a Clear Desk policy must be adhered to by all staff and managed by line managers (for more information please see Annex 2)

4.6 Using Personal Data

Personal data should only be processed for the specific purpose contained in the relevant privacy notice which was provided when the data was collected.

If staff wish to use the personal data in a new and unforeseen way the University Secretary's Office should be contacted to review the relevant Privacy Notice. If the change would not reasonably be expected by the data subjects, staff must actively communicate the revised privacy notice to them. In certain cases clear consent from the data subjects must be obtained before the personal data is used in the new way. Data Protection by Design and Default must be considered throughout the lifecycle of personal data.

Staff should be aware of the possible risk of unauthorised persons viewing personal data displayed on computer screens or in paper documents, particularly in open plan offices. Preventative measures such as; facing computer screens away from high traffic or public areas, and taking care not to leave documents containing personal data in view, should be taken. The use of privacy filters on computer screens should also be considered: a review of privacy filters should be considered by line managers.

4.7 Marketing

All marketing activities, including communications which involve processing personal data must be managed in accordance with both the GDPR and the Privacy and Electronic Communication Regulation (PECR). Unsolicited marketing activities involving messages sent by telephone, fax, email or text must conform to GDPR and PECR. If you process personal data for these purposes, you must consult with the University Secretary's Office before any activity takes place.

4.8 Sharing and Disclosing Personal Data

When personal data is shared between University departments for valid business reasons the data must be relevant and the minimum necessary to achieve the objective. Any sharing of documents containing personal data, including special category data, should be shared using Google Drive if it cannot be processed appropriately in the centrally managed system. Files and folders can be shared using links to documents rather than sent as an attachment.

Information must be protected in accordance with the University's **Information Classification Scheme**

The use of email is not recommended for the sharing of sensitive personal information.

- Highly restricted information (e.g. special category personal information such as medical data) must never be shared via email.
- Restricted information (e.g. personal data such as name and date of birth) should not be shared via email, particularly where there are larger numbers of data.

If email is the only means available for sharing information (which is unlikely to be the case) then that information must be appropriately protected with encryption.

Approved working practices

1) Use the appropriate centrally managed system
Wherever possible the sensitive information should not be taken out of centrally managed systems. This preserves both the integrity and confidentiality of the information.

If you need to share information with a colleague then you should direct them to view the relevant record in that system (e.g. ask them to log into MyTeam, eRecruitment, CIES). You should not download staff and student records for sharing outside of the systems.

2) Use preconfigured shared folders to collaborate
*** This should only be done if option 1 is not possible ***

The use of a shared file/folder in Google Drive or University storage that is configured to only allow access to those that have a need to access the information is approved. You can link to these files in an email if need be (as access is controlled by the Drive permissions).

It is very important that you only give access to those that have a clear need to do so.

3) Use an encrypted email attachment
*** This should only be done if option 1 and 2 are not possible ***

You must encrypt any email attachment containing sensitive information. This is described here: https://students.sheffield.ac.uk/it-services/information-security/encryption/email

You must never include the password for the attachment in the email that is being used to send the attachment.

If a file has to be shared as an attachment (e.g. due file type), it must be either password and/or encryption protected, using tools such as Zip compression software. When using a password to protect the data, it must be conveyed to the recipient in a separate message. Best practice is to relay the password by telephone to the intended recipient.

Following sharing, departments must assess whether any new use of data will be compatible with the purpose for which it was originally collected. If not, the data subjects may need to be made aware of the intention to use their data in this way and in some instances consent may be required. In addition the DPIA screening questions will need to be considered.

4.9 Retention and Disposal

Departments must also consider the retention and disposal of the shared information. Where the data is required for a single purpose the duplicate information should be destroyed after use. Where a permanent record is required, the department must establish a process to ensure the data continues to be held in line with the Data Protection Principles and the University Retention Schedule. Further guidance on sharing data internally is available from the University Secretary's Office.

4.10 Third Party Processing

In some instances the University is required, for mandatory or statutory reasons, to share information with certain third parties outside of the University. Personal data may also be shared with other third parties; if there is a clear and lawful purpose for doing so, if the data sharing is a proportionate means of achieving that purpose, and if the data sharing is transparent to the data subjects. Further guidance on sharing data with third parties is available from the University Secretary's Office. In most cases, where the sharing of data is regular, then an information sharing agreement between the parties is required. Template information sharing agreements can be obtained from the University Secretary's Office.

The University, as the controller, continues to remain liable for ensuring personal data is processed in compliance with the Data Protection Principles, when the processing is

undertaken by an external company or organisation (known as a data processor). Although the processor is now also liable for any inappropriate processing activities. If a department decides to outsource a data processing function, it must ensure a data processing agreement is in place before any activity is undertaken by the processor, on the controller's behalf. There is a necessity to provide assurance the data processor will meet their legal obligations as stipulated by relevant data protection legislation, which are known as 'sufficient guarantees'.

The University Secretary's Office must be made aware of any intention to engage a data processor so that up-to-date guidance can be provided to ensure all documents, including contracts are compliant with relevant data protection legislation. When finalised, a signed copy of the data processing agreement should be sent to the University Secretary's Office, this will form part of the University's Records of Processing Activity (ROPA).

Relevant data protection legislation allows the disclosure of personal data to authorised bodies, such as the Police and other organisations that have a crime prevention or law enforcement function. Staff who receive a request to disclose personal data for reasons relating to national security, crime prevention or taxation should contact the University Secretary's Office for advice to enable the request to be recorded and processed in accordance with University procedure.

In response to most other requests, staff must not disclose personal data, or particularly special category (sensitive) data, without the consent of the data subject. (However, in some cases consent may not be appropriate, and the University Secretary's Office should be contacted for assistance). If consent is received, staff must ensure that the data is given to the correct enquirer: for this reason disclosure should be made in writing and not by telephone. If a request for the disclosure of personal data is received, and consent has not been given by the data subject, the request should be sent to the University Secretary's Office to process appropriately.

If personal details are requested by a data subject or third party that is not provided as part of normal business, the individual requesting the data should be directed to the University Secretary's Office for advice on how to make a Subject Access Request (SAR). The University must respond to SARs within one month of their receipt.

4.11 Transferring Personal Data within the University

Any transfer of personal data must be done securely and in line with the University's Acceptable Use framework.

Email is not a secure method of communication and sending personal data via external email should be avoided unless it is: encrypted, with the password provided to the recipient by separate means (such as via telephone); by other encryption techniques; or by the use of a link to shared folders or Google Drive

While internal email (within the University's email system) is more secure, it is still advisable to consider encrypting attachments which contain data belonging to a large number of data

subjects, or sensitive personal data, in order to mitigate the risks associated with emails being sent or forwarded to unintended recipients.

Emails containing personal data should, have an appropriate subject heading, and explain clearly to the recipient; why they are being sent the information, and what they are expected to do with it.

Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important emails are correctly addressed and care is taken when using the 'Reply All', forwarding functions, or when copying others in to emails.

Personal email accounts must not be used to send or receive personal data for work purposes.

When sending personal data externally, by paper form, a Royal Mail tracking service or courier service must be used. If personal data is sent via Royal Mail, it is recommended the 'Special Delivery' service is used, particularly if Special Category data is being transferred.

When sending personal data internally in paper form, it should be sealed in an envelope marked 'confidential' and ideally hand-delivered to the recipient. If personal data is sent via the University's internal mail 'Internal Recorded' and the name of the sender is to be written on the top right-hand corner of the envelope.

4.12 Destroying Personal Data

Departments should adhere to the University's Record Retention Schedule for all data (including personal data) they hold and ensure it is destroyed when no longer required. The retention periods specified within privacy notices should be reflective of the University Records Retention Schedule, which is contained within the University's Records Management Policy. Further guidance about record retention schedules is available from the University Secretary's Office.

On destruction, personal data in paper form must be shredded and/or sealed in the confidential waste bags provided by the University. Personal data in electronic form should be deleted. Portable devices that hold personal data can be destroyed by IT Services if office shredders do not include this capability.

5 Reporting a Data Breach

It is important the University responds to data breaches quickly and effectively. A breach may arise from; a theft, a deliberate attack on University systems, unauthorised use of personal data, accidental loss, by disclosure (including emails, containing personal data being sent to the wrong recipient), or equipment failure. Data breaches should be reported to the University Secretary's Office and/or IT Services as soon as possible so mitigation techniques can be implemented quickly to limit any potential repercussions.

All initial contact must be made via telephone, to ensure a member of the University Secretary's Office or IT Services can respond as quickly as possible. The University

Secretary's Office has produced guidance (Annex 4) and this should be followed for all data breaches.

ANNEX 1 – The Data Protection Principles

"Personal data shall be:

• processed lawfully, fairly and in transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

• collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')

• adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

• accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

• 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for the purposes of archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

• processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

• the controller shall be responsible for, and be able to demonstrate compliance with, the first principle" ('accountability')"

ANNEX 2 - Clear Desk Policy

To improve the security and confidentiality of information the University is adopting a clear desk policy for all desks and work stations. The aims of the initiative are outlined below;

• To ensure all information containing personal data (including, but not limited to special category data), and confidential information is properly stored. This includes information in paper format, or on an electronic storage or hardware device.

• To help reduce the risk of unauthorised access, loss of, or damage to information during and outside of working hours (including when desks or workstations are left unattended) Whenever a desk or workstation is left unoccupied for an extended period of time, or at the end of the working day, then the following shall apply:-

1. All information which is confidential (commercially sensitive or contains personal data) must be removed from the desk/workstation and locked in a drawer or suitable filing cabinet. This should include all paper files and storage devices such as USB drives and CDs.

2. All information which is intended for confidential should be handled and destroyed in accordance with the University's guidance on confidential waste.

3. Laptops, tablets, and other hardware devices must be removed from desks and workstations and locked in a drawer or filing cabinet.

4. Keys for accessing drawers and filing cabinets, should never be left unattended on desks, and should be either locked in key cabinets or an alternative safe location.

5. All computers must be locked (Ctrl+Alt+Delete) when left unattended, and should be completely shut down at the end of the work day, or when unattended for long periods of time.

6. Printed documents which contain confidential (commercially sensitive or contains personal data) should be printed (using pull printers only) and removed from the printer immediately.

7. Filing cabinets containing confidential information (commercially sensitive or contains personal data) should be closed and locked at all times when not in use, or when left unattended.

8. Passwords should never be written down, especially not on sticky notes posted on or around a computer.

ANNEX 3 – Data Protection Impact Assessments

Data Protection Impact Assessment screening questions

1. Will the project involve the collection of new (or additional) types of information about individuals

2. Will the project compel individuals to provide information about themselves, before they can make use of the service provided

3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information including third party processors

4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used.

5. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics

6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

7. Is information about information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly.

8. Will the project require you to contact individuals in ways which they might find intrusive or expected or unexpected? (e.g. by e-mail or telephone)

9. Is there any automated decision making, this is where no involvement or final ratification by a human being.

Answering yes to any of these questions means a Data Protection Impact Assessment is required

ANNEX 4 – Data Breaches

1. Introduction

Data breaches can occur through human error or malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. This guidance note process for responding to any reported data security breach, to ensure the University act responsibly and protect its information assets as far as possible.

2. Aim

The aim of this guidance is to describe the University-wide response to any reported data breach incidents, and ensure that they are appropriately logged and managed. This will be achieved by adopting a standardised consistent approach to all reported incidents to ensure that:

- Incidents are reported in a timely manner and can be properly investigated,
- Incidents are handled by appropriately authorised and skilled personnel,
- Appropriate levels of University management are involved in response management,
- Incidents are recorded and documented,
- The impact of the incidents are understood and action is taken to prevent further damage,
- Evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny,
- External bodies or data subjects are informed as required,
- The incidents are dealt with in a timely manner and normal operations restored,
- The incidents are reviewed to identify improvements in policies and procedures.

3. Definition

A data breach is considered to be "any loss of, or unauthorised access to, University data". Examples of data breaches may include:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential University data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit

For the purposes of this guidance data breaches include both confirmed and suspected incidents that involve personal data. Personal data is defined as any data that can identify an individual.

4. Scope

This University guidance applies to all University information, regardless of format, and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the University. It is to be read in conjunction with the University's Information Security Policy and Data Protection Policy.

5. Responsibilities

5.1 Information users: All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

5.2 Heads of /Department: Heads of Departments are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

5.3 Contact Details: The University Secretary's Office (USO), who will be investigating breaches and suspected breaches, can be contacted via dataprotection@sheffield.ac.uk

6. Data Classification

Data breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the University is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

6.1 **Public Data**: Information intended for public use, or information which can be made public without any negative impact for the University

6.2 **Internal Data:** Information regarding the day-to-day business and academic operations of the University. Primarily for staff and student use, though some information may be useful to third parties who work with the University.

6.3 **Restricted Data**: Information of a more sensitive nature for the business and academic operations of the University, representing the basic intellectual capital and knowledge. Access should be limited to only those people that need to know as part of their role within the University.

6.4 **Highly Restricted Data**: Information that, if released, will cause significant damage to the University's business activities or reputation, or would lead to breach of the Data Protection Act. Access to this information should be highly restricted.

7. Data Security Breach Reporting

Confirmed or suspected data security breaches should be reported promptly to the University Secretary's Office (USO), email: dataprotection@sheffield.ac.uk the report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible the incident report form should be completed as part of the reporting process. See Appendix 1. Once a data breach has been reported an initial assessment will be made to establish the severity of the breach.

All data security breaches will be centrally logged by the USO to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

8. Data Breach Management Plan

The management response to any reported data security breach will involve the following four elements. See Appendix 2 for Investigation pro-forma

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

9. Authority

Staff, students, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

10. Review

The USO will monitor the effectiveness of this guidance and carry out regular reviews of all reported breaches.

Incident Reporting Form

Please act promptly to report any data breaches (or potential data breaches/near miss). If you discover a data breach or near miss please notify your head of department and complete and return the form below to dataprotection@sheffield.ac.uk

Description of breach:	
Time data breach was identified and by whom:	
Time data breach occurred and by whom:	
Who is reporting the breach?	
Name/post/department:	
Email address:	
Classification of data breached (in accordance with the universities breach policy): i. Public data ii. Internal data iii. Restricted Data iv. Confidential Data	
Volume of data involved (number of people effected):	
Is the breach contained or ongoing?	
What actions are being/have been taken to recover the data?	
Any other relevant information:	

Please email this completed form to dataprotection@sheffield.ac.uk.

To be completed by the USO and, where applicable, in consultation with IT Services.

Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
How many data subjects are affected?	
Does the data relate to any contractual arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories: **HIGH RISK personal data Sensitive personal data (as defined in the Data Protection Act) relating to a living, identifiable individual's** **a) racial or ethnic origin;** **b) political opinions or religious or philosophical beliefs;** **c) membership of a trade union;** **d) physical or mental health or condition or sexual life;** **e) commission or alleged commission of any offence; *or*** **f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.**	
Data Protection Officer and/or Lead Investigation Officer to consider whether it should be escalated to the appropriate University Executive Board member.	
Have the ICO been Notified? Explain decision.	