Data Protection Policy

Version:	5.1
Dated:	06 November 2023
Document Owner:	Information Governance Manager & Data Protection Officer

Revision History

Version	Date	Revision Author	Summary of Changes
V4	October 2022	Brenda Waterman	**Document creation** *This policy incorporates previous policies:* Information sharing Policy, DPIA Policy, Password Policy, Privacy and Personal Data Protection Policy **New items:** • Training • Staff • Remote working • Sharing data internally • Police requests • Research • Secure Data Research Hub • Protecting data with security • What happens to your data when you leave
V5	November 2022	Brenda Waterman	Research update Changes to Roles and Responsibilities
V5.1	October 2023	Brenda Waterman/Rick Cockram	Update to new branding and inclusion of information security tooling details. Amendments to text providing more details reflective of business and case law

Document Approval

Version	Next Review Date	Governance Group	Approval by
V4	October 2020	Information Steering Group	Andrew Connolly
V5	December 2022	Information Steering Group	Andrew Connolly
V5.1	November 2023	Information Steering Group	Linda Peka

Table of Contents

Definitions

SDRH	Secure Data Research Hub
DSPT	Digital Security, Privacy Toolkit - NHS
ISO27001	Certification of Security standard – Information and security Standard
IG	Information Governance
SIRO	Senior Information Risk Officer (UK DPA/GDPR)
DPA	Data Protection Act
GDPR	General Data Protection Regulation
FOI	Freedom of Information Act
PECr	Personal Electronic Communications regulation
NCSC	National Cyber Security Center

1. Introduction

The University of Exeter is fully committed to protecting all data of its students, employees, suppliers, and other stakeholders in accordance with the requirements of the Data Protection Act 2018(UK GDPR) and other related legislation such as Personal Electronic Communications Regulation and Network Information Systems.

The University of Exeter is the 'data controller' and the Council of the University, as the governing body, is responsible for compliance with current data protection and related legislation. The University will take the appropriate measures to ensure the protection of all data, through training, guidance, and due diligence, by ensuring privacy by design, data subject's rights, and security is upheld to protect the infrastructure and data within.

The University is required to employ a Data Protection Officer to provide independent advice and oversee the protection and security of data in line with the DPA 2018 (UK GDPR).

More information can be found in the Information Governance and Data Protection Framework.

This Policy sets out the core obligations of the University and its staff in handling personal data. References and links to other documents are included which provide more details where required.

The Data Protection Officer and the Information Governance Team are responsible for ensuring the University is compliant and works with all parts of the university providing advice and collaboration.

Data and information are valuable resource and should be protected. Under the Data Protection Act data is identified as Personal or Sensitive data that is collected, processed, stored, and shared where any part can identify an individual, this could include an IP address or cookie identifier. This can also include a combination of data fields that together can identify the individual.

All data collected and held by the University of Exeter, or a third party on their behalf, is subject to individuals' rights under the Data Protection Act 2018/UK GDPR, Freedom of Information Act and Personal Electronic Communications Regulations.

2. Policy and Approval Process

All relevant Policies that are in place to protect the privacy and security of data are approved by the Information Steering Group. This group meets three times a year and is chaired by the appointed Senior Information Risk Officer. Membership consists of University Directors or their delegates. Terms of Reference can be requested via Information Governance.

Policies relating to the Privacy or Security of data can be submitted at any time for approval by the group. This can be given with at least a quorum of senior staff members, including the chair.

All policies will be added to the agenda of the next meeting to be formally minted, along with evidence of those who approved.

All policies should state the version number, date of approval, date of review, the person responsible for the Policy, and summary of changes.

Directors and Assistant Directors will be notified of all approved policies and are responsible for ensuring staff awareness.

3. Roles and Responsibilities

3.1 All staff

All individuals making use of the University of Exeter's information assets are responsible for ensuring that they are aware of the requirements of the University's policies in relation to information governance, data protection and data security, and adhere to them as they relate to their use of The University's information.

All users are responsible for highlighting areas of perceived risk or where information practices could be improved to their line managers and/or Information Governance.

All users are responsible for reporting any incidents that could be considered a breach of personal data that is processed by the University's and breaches of University policies, or legislation to the Data Protection Officer, Manager or Senior staff by contacting information-security@exeter.ac.uk or informationgovernance@exeter.ac.uk.

3.1.1 Contractual obligations

All staff, Associates and temporary staff are bound to confidentiality obligations as described in their terms of employment. Other individuals may be required to enter confidentiality obligations with the University.

3.1.2 Disciplinary procedures

Any breach of confidentiality in line with the University's information governance and data protection and security policies may result in disciplinary action including, in the most severe cases, termination of an individual's employment or engagement by the University.

3.1.3 Security Checks

Some staff working on confidential or special category data may be required to have DBS or other security checks undertaken as required by the role or under contractual obligation by a third party (for example, research funding). Details of security checks can be found for Staff or Students on the website.

3.1.4 Mandatory Training

All staff and associates must complete mandatory training within one week of commencing employment. For further information, see our web pages: Mandatory Training.

All mandatory training is monitored and if it is found that staff or associates have not completed the training, action may be taken in accordance with HR and other probationary procedures. If any member of staff or associate has difficulty accessing the training, they must contact the Organisational Development Team.

Dispensation may be granted where the following is provided:

- Evidence of undertaking equivalent Data Protection training from another employer.
- Content of the sections covered in the training.
- Training undertaken within the last 12 months.
- Individuals may be requested to re-do mandatory training or 'bite-size' training following a breach of personal data.

4. Staff who require access to the Secure Data Research Hub

It is a requirement to meet Digital NHS, ISO27001, CE+, contractual and other regulatory requirements and that additional mandatory training is undertaken to enable access to the SDRH.

Users who are required to access SDRH are required to complete Researcher training found via LearnUpon.

On completion of the Data Protection Impact Assessment and other relevant documents, Information Governance and Security mandatory training and SDRH training, access will be given.

There are also other obligations by requirement of contract, or heightened security due to research topic, in which additional compliance training requirements are required of staff. These requirements can be specified in a research contract or sharing agreement, or in a statutory requirement for clinical trials or genetic research.

Information Governance staff can provide bespoke training upon request from any part of the University: contact InformationGovernance

5. Roles

5.1 Senior Information, Risk Officer (SIRO)

The appointed SIRO is the Deputy Registrar and Executive Divisional Director of Education and Academic Services. They are the chair of the Information Steering Group Chair and hold monthly meetings with DPO. It is part of the legislation that the DPO should report to the senior manager who reports to executive boards the SIRO meets this requirement. It is the responsibility of the DPO to alert the SIRO and the Registrar of risks, breaches, or circumstances that can create a risk to data or potential damage to the University's reputation.

5.2 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is a statutory role and is empowered to ensure, in an independent manner, that the University meets the requirements of the Data Protection Act 2018 /UK GDPR and other related regulatory requirements. The DPO is based within UCS, and is line managed by the Assistant Director of CGR. There are also reporting lines to the Director of IT Services. The role and functions of the DPO are defined within legislation and are in addition to the responsibilities of the Information Governance Manager.

5.3 Registrar

Named Controller and assurance of DPO processes. The Controller is responsible for all processing of personal data across the university, of which the DPO must ensure meets all aspects of the Data Protection Act.

5.4 Director of Exeter IT Services

Collaboration with security and projects, to be made aware of risks to security and take remedial action or advise of future developments. To advise the DPO of Cyber security risks, incidents and potential risks that endanger the security of data held by the University.

5.5 Divisional Director of University Corporate Services

Ensure suitable resources are allocated to the DPO and IG team to enable the team to fulfil their role and responsibility in line with the relevant legislation.

5.6 General Counsel (including HR)

Collaboration over Legalities and contracts, it is their role to support, advise and consult with the DPO on issues that may affect or present a risk to the University's data.

To provide advice on legal issues relating to casework and litigious complaints.

5.7 Assistant Director of University Corporate Services

Line management Information Governance Manager & DPO. It is their role to have oversight of SDRH, responsible for managing the accreditation requirements for ISO27001 and the Information Security Management System ISMS.

5.8 Head of IT Security Operations

Collaboration on security and cybersecurity matters. It is their role to engage and inform the DPO on matters of security and threat intelligence.

5.9 Research IT Manager SDRH

Collaboration on the Security and processing as well as maintaining records of onboarding research into the Secure Data Research Hub.

5.10 All Line Managers

- Ensure all staff within your remit have completed mandatory training and refresher training.
- Staff must be given time to undertake mandatory training relevant to their post.
- You should not 'pass on' a laptop from a previous staff member unless 're-built' by IT. The laptop may have links and personal data on it.
- When a staff member leaves, it is the manager's responsibility to ensure that work-related emails are stored as required if continued access by the team is required.
- When an individual leaves, if they have 'shares or documents of importance stored, ensure that they are not in OneDrive or within an email folder.
- Must ensure data is handled and stored in accordance with legislation and the purpose it was collected for. See 8 below.

6. What is Personal Data?

Any Data that can identify an individual. This can be common identifiers such as name, address, phone number, email address, Identification numbers such as staff number, patient number, location such as GPS via phone, an online identifier, cookies, photographic media, employment details, DNA, passport number, blood group, social economic status - the list continues, although some would have to be with other factors. In today's society, nearly everything we do can leave an identity marker of some kind that can be traced back to an individual.

The Data Protection Act breaks data into two categories:

- **Personal Data:** Name, Address, DOB, phone number and similar
- **Special Category Data (SCD):** racial or ethnic, political opinions, religious or philosophical beliefs, membership of groups such as Freemasons, genetic, biometric, health, sexual orientation, criminal record (Law Enforcement Act).

6.1 Key points

- You must have a reason to collect personal data: see item 8 below.

- It is important that any data collected is stored and protected appropriately, particularly any that comes under additional requirements or who have contractual clauses. This is covered as part of the Data Protection Impact assessment: see item 14 of this policy.
- Where AI is being used extra caution must be given such as impact to individual(s), bias, and harm.

In addition to protecting Personal and Special Category Data, to meet the UK Data Protection Law, it is important to recognise that the University may hold **Commercially Sensitive** data that needs protecting too. More information can be found here: Records Management.

7. Reasons for Collecting Personal or Special Category Data

All data collected and held must be processed Lawfully, Fairly, and Transparently to meet the requirements of the Data Protection Act (DPA).

- You must be able to provide a clear detail of what data you are collecting and why it is required.
- You must only collect and process data to meet the purpose and not collect 'just in case we need it'.
- Data must be stored securely with appropriate access controls on who has access.
- Data must not be used for another purpose for which it was obtained.
- Data must be protected following the security policies of the University.
- Special category data requires extra security.
- Some data requires extra protection: NHS data, or data requiring meeting contractual requirements or CE+ or ISO27001. If your data requires any of these it must be stored within the Secure Data Research Hub.
- Data processed using AI must identify its purpose and impact including and decision making processes.

To ensure the university is meeting these requirements a Data Protection Impact Assessment (DPIA) must be completed to demonstrate compliance with the UK DPA but also to meet the other requirements as above. Where appropriate this will also include third party supplier questionnaire which IG will provide with the DPIA, these must be completed by the supplier and returned.

The Secure Data Research Hub (SDRH) is a cloud-based platform where certain types of Research data are hosted. This is required to meet regulatory and certification compliance. If your DPIA indicates that your data must be in the SDRH, you will be required to undertake specific steps and training to do this. Please note fees apply if storage is required within the SDRH.

8. Remote Working

It is the individuals' responsibility to ensure University of Exeter data and equipment is protected when working off site. With staff working in Hybrid contracts, it is ever more important that care is taken to protect the equipment and data it may hold.

- Your equipment must have security in place to protect the infrastructure and the data held BitLocker, MFA, secure Password.
- It is your responsibility to install updates and protect data as required by Exeter IT security. Microsoft alerts will show on your screen to install.

- New applications can only be installed with permission through either the DPIA process or Exeter IT and should be accessed via single sign-on only.
- No portable storage devices are to be used to store data unless it is fully encrypted meeting Exeter IT requirements. Staff requesting these should consider other alternative more secure storage methods for portable data such as SharePoint.
- You should not allow non-staff to use your equipment.
- You should not share your login details.
- When you have finished work your laptop /PC must be closed.
- When connecting from public/untrusted networks, you should setup a secure connection to the University VPN service before transmitting. This mitigates the risk of cyberattacks and other security threats.
- When working in public environments you must not leave your laptop in a vulnerable place or work where you can be overlooked (e.g., train). If this is a regular occurrence that cannot be prevented talk to Exeter IT regarding a privacy screen cover for your laptop.
- Teams calls, where discussing sensitive or individuals must not be in a public place.
- Paper documents must not be left in places that can be easily seen and should be stored in secure locations appropriate to the content or as specified in contractual obligations.
- Clear desk practice should be adhered to when leaving your working environment at all times. Any documentation (electronic or hard copy) relating to the University of Exeter including research should not be left visible on your desk or screen for others to view.
- All hard copy documents must be securely destroyed.
- All equipment to be returned to the University of Exeter either to your manager or directly to Exeter IT at the point of leaving employment, as agreed with your manager.

Information Governance Related policies and Guidance (Internal)

9. Data Subjects Rights

All data subjects have rights to request their data these fall under the following categories:

- The Right of Access
- Rectification
- Rights of Object
- Right to object to direct marketing
- Right to erasure
- Right to restrict processing
- Automated decision processing
- Data portability

If you receive a request for this type of action, you must report it to the Information Governance (IG) team.

Each category has a specific process within the Data Protection Act – failure to adhere to these processes can result in complaints to the ICO, and possible fines and /or audits. Exceptions for some types of data requests are in place: see Information Governance Related policies and Guidance (Internal)

- If you are requested to provide data to meet these rights, you must follow the guidance provided within the request from IG.

- All relevant data must be supplied to IG who will redact and collate the data following the legislation.
- You must not pass this data directly to the requestor unless discussed with IG officer or in line with the IG guidance document.
- Documents/emails are only likely to be 'Legally Privileged' if:
    - the email 'To' has a recognised Legal person's name who is in a position to advise and is named within the organisation (General Counsel)
    - Email is requesting either legal opinions, advice, or suggestions to the General Counsel or HR General Counsel
    - If it becomes part of an email trail, it can lose the Legal Privilege protection.
    - if in doubt ask legal or provide the information and IG will liaise with legal and apply the rules to remove or redact appropriately.
- Data requested can be in many forms, Email, CCTV, documents, systems, teams, video, and audio, and can come from anywhere in the University.

10. Sharing Data Internally

The University will only share your data for specific purposes in line with the UK DPA 2018 (UK GDPR), more details on this can be found in our Record of Processing Assessment.

- Data shared must be aligned for the purpose it was collected. For example, if data is collected for registration, it cannot be used for research or marketing.
- If data is required by another area of the business to use for a different purpose other than what it was collected for. Please contact Information Governance.
- A fine line exists between using the data for analysis to inform the business and to meet legal, regulatory requirements or evidence of processing; and allowing the data to be used for research or another function other than what it was collected for. Information Governance officers and DPO can advise on these matters.

11. Breaches

A breach is defined as:

'a breach of security or process that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data'
- (Information Commissioners Office).

This includes breaches that are accidental, deliberate or caused through Phishing /Cyberattacks.

- You must wherever possible share documents (rather than send by email).You can share via SharePoint.
- If a breach has occurred report it immediately to SID and contact the Information Governance team via email at informationgovernance@exeter.ac.uk (should this be information-security@exeter.ac.uk?)
- IG and IT will undertake remedial action to protect the data and advise you or your manager to undertake further action to protect the data.
- Information Governance will assess the risk of the breach and alert the DPO.

- The DPO will undertake a formal investigation to report to the Information Commissioners Office, third parties and data subjects or to comply with contractual obligations.
- The process that caused the breach will be reviewed and the DPO and Head of IT Operational Security will take remedial action or proposals in process to mitigate the risk of further breaches.
- Breaches of Security and Data Protection out of hours should be reported via SID. This will be picked up by IT Security and DPO as appropriate.

11.1 Secure Data Research Hub

In addition to above, within the Secure Data Research Hub, a log of all potential breaches is required including security threats, to meet the DSPT, Certification, regulatory and contractual requirements.

- The DPO will report to Digital NHS and where appropriate and third parties where applicable by contract.
- The Lead Researcher may also be required to notify 3rd parties dependent on contracts.
- The DPO will maintain a log as evidence for ICO, NHS and 3rd parties of the breach and remedial action taken.

12. Police Requests

Police can request data under the Police Reform Act 2002. A formal request is required via email from the officer requesting. The form should state the reason of the request and details of what is required. These requests should be forwarded to Information Governance /DPO in accordance with legislation or contractual requirements.

There are some exceptions to this, such as an emergency situation that requires direct action or for the vital interest of an individual. This can include evacuation of a building or a serious accident. In these cases, IG should be contacted as soon as possible.

- If you receive a request either through email or phone, please contact Information Governance via email. In the case of phone calls clarification of the person is required.
- All requests for data must be proportionate to the event being investigated.
- The Police can request many differing types of data. IG ensure the data is relevant and answers the request, seeking clarification where required.
- The Information Governance Officers or DPO will provide a formal response to the Police.

13. Data Protection Impact Assessments (DPIA)

The DPIA is required for any new system, new processing, collection of data, or changes of use, use of AI or data sharing. It is important that you contact IG/DPO early in the project bid or planning.

If you are carrying out system upgrades, introducing new data fields, reorganising the structure of data, upgrades or new security systems or any changes to processing you must complete a DPIA.

The DPIA investigates information required under the UK DPA 2018/ UK GDPR - Data by design and Default:

- What are the objectives of the Project – why does it need to collect data?
- What type of data is being collected?

- How are we collecting the data?
- What will the data be used for – its purpose?
- How will the data be processed?
- Where and how will it be stored
- What hardware, software, networks will be used
- Who will be processing the data?
- Is the data being processed using AI?
- Is the data pseudonymised, anonymised or collated with other data?
- If data is already collected how is the new processing different
- What 3rd parties are involved; do they use sub-processors?
- How long will the data be kept, and how will it be destroyed?
- Are international transfers of data agreements required?
- As part of this process IT processes are required for funding, project management, procurement etc – in line with regulatory and Audit requirements.
- Third Party supplier questionnaire for suppliers to complete.
- The DPO, IG will review DPIA
- IT Security will sign off 3rd party supplier questionnaire for security and the DPO will sign of the final document with advisory notices, notification will be sent to the project manager, asset owner and other relevant persons to inform when the DPO has signed off.

As part of this process IG will provide:

- Privacy statements, update Record of Processing, liaise with Legal for Sharing Agreements, International Data Transfer Agreements, contractual conditions for FOI, identifying risks and mitigations.
- Advice on completion of the form and on sensitive data
- Advice on meeting contractual obligations

All data being stored within the SDRH must have a DPIA completed and signed off by the DPO prior to gaining access.

14. Minimisation, Accuracy, Data Definition

When Staff are defining and using data it is important that the following rules are adhered to:

- Data must follow the minimisation rule meaning that data collection must be fit for purpose and cannot be collected 'just in case'.
- Data minimisation also means that the university should not be duplicating collection of the same data. Wherever possible duplication should be avoided. It is a risk that either system could have incorrect data.
- Data must be kept accurate. Failure to update new addresses and information would be deemed a breach of individuals' data and can be reported to the ICO which could result in fines and damage to reputation.
- Data definitions and labels should be consistent across the university for key data fields. For example
    - System one: Gender: Male, Female, Other.
    - System two: Gender Identity: Male, Female, Transgender Man, Transgender Female, Binary, Bi gender.

This enables clarity on reporting, creating consistent data sets for HESA or other regulatory returns. The Business Intelligence Team will be able to advise on correct data field categories.

15. Retention, Classification and Assets

As part of the Data Protection Act the university must maintain an asset register of processing, applications, retention, and classifications, these can vary dependent on usage and requirements of the data set.

15.1 Retention

It is the responsibility of all staff to ensure that documents, emails, research data etc. is not kept for longer than required this applies to hard copy as well as electronic data.

- The University Retention Schedule should be reviewed by data holders at least annually.
- When new processing is introduced a new row on the schedule of retention must be added
- Managers and Information Governance must review the Retention Schedule annually.
- It is the responsibility of the data owners to ensure data is deleted inline with the retention schedule.

15.2 Classification

- Data classification allows controls on the documents that will trigger extra security through email and storage.
- Users should use appropriate labels for added security where available.
- SDRH by definition of data type and contractual requirements means all documents meet the classification of Confidential as defined below:

Confidential	High Poses an immediate or significant risk to the reputation and or financial position of the University or a third party. Would result in a severe privacy breach or breach of confidentiality. *Government equivalent: Official - Sensitive*	Information to which access is strictly controlled and restricted only to predetermined, approved groups or members of University of Exeter staff by name or role. Information must be stored in locations with security appropriate to the sensitivity of the data.	• Special category personal data of identifiable individuals. • Bank details and financial information • Transcripts and exam papers • University IP including course content and unpublished research data • Investigations, & disciplinary proceedings • Commercially sensitive information

- For more information on classifications see Information & records Management Policy

15.3 Assets

The university is required under the UK DPA/GDPR to maintain an Asset register of all processing activities with information relating to systems, lawful reason of processing, Information Asset owner, and location data is held among other items. Information Governance are responsible for managing this process. IntoZetta is an electronic system that will meet these requirements as well as Data mapping and Data accuracy on key systems.

- Asset registers must be updated annually.
- Information Governance will remind Asset Owners to appoint appropriate staff (managers) to review and update the register.
- Information asset owners will receive Reports to understand the assets and processes they are responsible for (these will be available 2024 from IntoZetta)

More details can be found on our Information and Records Management site

16. Records of Processing

It is a requirement of the DPA 2018 that organisations must be transparent in processing. One of the ways this can be achieved is through a Record of Processing.

The document must include:

- A list of our processing activities
- What business function do we fulfil?
- Lawful reason of processing
- Data types
- Where the data is stored
- Link to Retention schedule
- References to privacy notices and the rights to individuals
- The systems we use to collect data.

Staff must inform Information Governance of changes to processing or changes in systems to enable this document to be kept up to date.

The University Asset register should be reviewed and maintained annually and update the Record of Processing.

17. Research Data

Research data is a significant part of the data collected by the University. Research data has many controls in place by Information Governance, Ethics, and other regulatory plus contractual requirements by funders and/or partners.

- The DPIA applies to this data too, including contracts, sharing agreements, storage, and access.
- The lawfulness of processing will inevitably be Consent from the individual to participate in the research, but the data collected from the participant will usually be 'in the public interest'. You must discuss with IG or ethics in determining this distinction.
- Research Data can also be subject to audit by third parties / Collaborators.
- Research data is a valuable asset and must be kept secure. It is important that where data includes sensitive data, it is stored securely within the University infrastructure.
- The options open to store data are SharePoint, Research Data Storage, Secure Data Research Hub. All have varying degrees of security. The SDRH meets NHS controls and ISO27001, CE+. Your DPIA will determine how you need to store your data.

18. Secure Data Research Hub

Enhanced controls are in place to meet a higher level of security. Data can range from limited personal data where the supplier requires a higher level of security, to special category data or where particular security standards are required to meet DSPT, ISO 27001, CE+ or determined by contract or classification level.

- It is important that staff start the process of DPIA as early as possible, before going to Ethics, as this will identify the requirements of the project and the costs of storage. Staff will not get access to SDRH unless a DPIA has been completed. This will identify any privacy statements required and be included in the completion of the document.

- If the research project requires a higher level of security, then you will need to complete a form to notify Research IT and to work out the storage costs. Details can be found on the Research Data Management where the form can be found to complete.
- IG and Security mandatory training must have been undertaken as well as SDRH training: both must be completed before access is allowed. Training is monitored, and failure to meet this requirement will impact on your ability to access the SDRH.
- If third parties are required to access, they will be set up with associate accounts and will be required to complete the training.
- It is the obligation of the Lead Researcher to set up the user levels within the SDRH for the project. They are responsible for ensuring that staff listed against a project is kept accurate.
- Information on the requirements of users and lead researchers will be set out in the training.
- The lead researcher is responsible for allocating the specific security controls to the specific staff within the project.
- The SDRH is built to allow you to work within the virtual desktop environment and has some standard applications loaded. More can be added if requested and security checks are completed and approved.
- Downloading data should be limited and not copied onto portable equipment. Data is not deemed compliant to standard if no longer held in the SDRH. If you have this requirement, please contact IT Research Manager and Information Governance Manager/DPO.
- The SDRH has backups that happen during the Day, Monthly and Annually which is retained for one year.
- All elements of the UK Data Protection Act/GDPR apply:
    - Lawfulness of processing – due to the nature of research this is most likely to be 'in the public interest' article 6
    - International Data transfers and sharing agreements article 46
    - Data Minimisation & Retention articles 4, 5
    - Data by Design & Default article 25
    - Other areas of the DPA may apply depending on data set and project.
- All Policies relating to the protection of data, including security must be approved via Information Steering Group and be reviewed annually.

19. Equipment

The University provides equipment to Staff to facilitate functions of employment. These include Laptops, tablets, phones, USBs, NAS drives, Wi-Fi dongles, and assistive technology. Any equipment that has been provided by the university that can hold personal data must be protected and not shared or used by unauthorised parties.

Staff or associates that have been issued with equipment are responsible for ensuring it is stored and used appropriately to protect the equipment and content.

- Mobile devices should not be left unattended in unsafe environments or where they can be overlooked; for example, coffee bars, trains or open areas within the University premises.
- Staff must always take appropriate precautions to protect the equipment and any data including physical storage or paper held against theft, or accidental damage including

unsafe environments. This includes home working or visiting other Universities or attending any external meetings, conferences etc.

- When you have finished working on your laptop, it should be shut down for the day, including any portable storage or physical documentation, and placed in a secure location such as a secure drawer of cupboard. This applies to all working environments.
- Portable storage supplied by the university should be adequately protected with BitLocker, MFA, secure passwords, encryption. Following IT Security policies.
- If you lose your equipment, you should notify Exeter IT, Information Governance immediately and your manager.
- If travelling with your equipment it is important that it is secured within the boot of your vehicle, or securely in a bag. You must not leave your equipment unattended at any time.
- It is the responsibility of managers and individuals to ensure equipment is returned to the university upon leaving employment.
- Where equipment has come to end of life you should contact Exeter IT who will arrange for secure disposal of equipment.

20. Protecting Data with Security

Everyone is responsible to ensure data is secure:

- Passwords should be maintained to meet the University Password Policy. Passwords should not be shared.
- All users are required to install and use BitLocker and MFA.
- Ensure you have screensaver enabled to protect your equipment when you walk away.
- Be cautious when opening unexpected or external emails. Check the email address it was sent from. B.Anyone@exeter.ac.uk is very similar to B.Anyone.exeter@gmail.com at first glance.
- Do not click on links with a suspicious links in them.
- Be cautious with callers who are asking for information. In a call, can you be sure that they are the data owner/subject?
- Ensure you close your laptop when not using it.
- If you have any doubts about an email you receive, email or call to inform Exeter IT or Information Governance.
- Maintain your laptop and equipment with updates as advised by Exeter IT

In some research projects and staff positions security checks will be required, this can be done via an application to HR.

As part of this process Exeter IT and the DPO will use compliance tools to monitor and audit Compliance logs available within the infrastructure. These will include but not be limited to the monitoring of storage and communications channels using Data Loss Prevention tools example to alert when emails are being sent with attachments that have personal or sensitive data within them, data searches using tools provided in Microsoft Purview, and enforcement of the classification policy through marking using Sensitivity Labels and other technologies where available. Information Governance and IT Security will review the use of these tools in collaboration with business areas to ensure the level of protection and level of effort are in balance.

21. What Happens When You Leave?

Security and Confidentiality remains in place and your email and OneDrive or other storage locations with no longer be available for you to access and will be deleted in line with the corporate retention schedule.

- On leaving, user accounts are closed. Individuals will not be able to access the university's infrastructure.
- An ex-staff member will not be able to access the network, email, or OneDrive from this point.
- Any shares to email or OneDrive will cease upon departure.
- The contents of these items will be permanently deleted 3 months after a departure.
- University confidentiality clauses continue after leaving from both employment and potential 3rd party contract.
- All equipment should be returned prior to the leaving date.

22. Related Policies

- HR website links
- DBS Baring
- Confidentiality
- Security specific policies
- IG policies and guidance
- Information Governance and Data Protection Framework.
- Records Management

23. Policy Monitoring & Desktop Audits

Annually the DPO will measure the effectiveness of this policy by testing key elements of the requirements. The results will be reported to the Information Steering Group, and where required, other groups and the University Compliance Committee and an action plan will be created to address any gaps in compliance.

The monitoring will include, but not limited to:

1	A review of mandatory training compliance
2	A review of SDRH mandatory training compliance
3	Sample survey of data owners: • Collecting data according to DPIA • Use of data in accordance with DPIA • Remote working security • Sharing data internally • Processing of data is aligned with legislation, contracts
4	Distribution of reported security weaknesses, incidents, and breeches