University of Essex

Information Security Policy

Authors:	Information Assurance Team
Publication date:	December 2022
Amended:	December 2024
Review date:	December 2025

Table of Contents

1. Introduction

The University of Essex is a knowledge organisation; our contribution to society is through the knowledge that we explore, create and convey. Information is the currency for our production and propagation of knowledge; credible academic or professional activity cannot be conducted without reference or access to it.

2. Purpose and scope

This policy provides a framework for the management of information security throughout the University. It applies to:

a) all those with access to University information systems, including staff, students, visitors and contractors

b) any systems attached to the University computer or telephone networks and any systems supplied by the University

c) all information or data[1] processed by the University pursuant to its operational activities, whether processed electronically or in paper (hard copy) form, and including any communications sent to or from the University and any University information or data held on systems external to the University's network

d) systems or information accessed remotely or via mobile devices

e) all external parties that provide services to the University in respect of information processing facilities and business activities, and

f) principal information assets including the physical locations from which the University operates

The policy applies equally to all areas of the University, although some areas will have their own additional requirements.

---

[1] While information and data are not synonymous terms, they are often used interchangeably and are closely connected. The security of both is important: security of data often underlies and informs security of information since data underlies information. This document generally uses the term "information" but that should be taken to include data.

The policy is supported by other relevant University polices and guidance (see Section 7, below). Help and advice on the practical implementation of this policy is available.

3. Aims and commitments

The University recognises the role of information security in ensuring that users have access to the information they require in order to carry out their work. Information underpins all the University's activities, and is essential to its research, teaching, commercial and administrative functions. People working with information need to be skilled and supported in handling it correctly. Much information is handled electronically, and the University makes extensive use of information systems to manage its information.

There are two key areas of risk related to information. The first is any reduction in the confidentiality, integrity or availability of information which could prevent the University from functioning effectively and efficiently. The second is the loss or unauthorised disclosure of information which has the potential to damage the University's reputation and cause financial loss. Loss of information in some circumstances may attract financial penalties.

To mitigate these risks, information security must be an integral part of information management, no matter the form in which the information is held.

The University is committed to protecting the security of its information and information systems in order to ensure that:

a) the integrity of information is maintained, so that it is accurate, up to date and fit for purpose

b) information is available to those who need it, when they need it

c) confidentiality is not breached, so that information is accessed only by those authorised to do so

d) the University meets all its legal and statutory requirements, and

e) the reputation of the University is safeguarded

In order to meet these aims, the University is committed to implementing risk-based security controls. Information and information systems both feature in the University's approach to risk management and are listed in the University's operational risk register.

Information security risk assessments will be performed for all information assets on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.

As part of the University's information culture all University students and staff will know how to access information and understand their responsibilities. They will be supported to be able to assess risk, take responsibility when things go wrong, and put things right quickly.

The Cyber Security Programme Board reviews the University's strategic approach to information security. The Information Security Management Group within Digital Innovation and Technology Services reviews the detail of the University's technical approach to managing threats to information security. Mechanisms are in place to assess and address any breaches of information security.

Both the Cyber Security Programme Board and the Data Protection Officer submit regular reports to the University's Audit and Risk Management Committee on matters within their remits.

4. Responsibilities

4.1 Council

Council has ultimate responsibility for risks to the University, including those relating to information security and compliance with legislation and the expectations of regulators.

4.2 University Steering Group

The Registrar and Secretary, as Senior Information Risk Owner (SIRO), is the principal officer of the senior executive team (University Steering Group - USG), with responsibility for information security. The Registrar and Secretary is advised on relevant matters by the Data Protection Officer, the Deputy University Secretary, and the Chief Information Officer. The Registrar and Secretary is responsible for:

a) ensuring that the integrity of information is maintained, so that it is accurate, up to date and fit for purpose

b) ensuring that users are aware of this policy

c) seeking adequate resources for its implementation

d) monitoring compliance

e) overseeing regular reviews of the policy, having regard to any relevant changes in legislation, organisational policies and contractual obligations, and

f) ensuring there is clear direction and visible management support for security initiatives

4.3 Information Assurance Manager and Data Protection Officer

The Information Assurance Manager, as Data Protection Officer, provides advice and guidance on compliance with data protection law.

4.4 Heads of Section, Schools, Departments and Centres

Heads of Section and Heads of Departments, Schools, Centres and Institutes are responsible for ensuring that their functional areas comply with the University's information security requirements and have effective systems in place for managing information security in accordance with this policy and any supporting documentation and guidance.

4.5 Information champions

Every section, department, school, centre and institute has a designated Information Champion. Information Champions may be academic or professional services members of staff. This University-wide network provides a focal point for information security in sections, departments, centres and institutes sharing good practice, providing practical advice, signposting staff to further advice and support, and monitoring and reporting problems. Information Champions support Heads in meeting their information security responsibilities.

4.6 University members

Every member of the University, including staff and students, and others granted access to University information or systems, has a responsibility for the safe use of information and information systems used in support of their University role, and for working within the appropriate policies, procedures and structures that are in place to safeguard the security of information.

All members of staff are required to complete the essential training provided by the University; this includes mandatory training, including an annual booster, on information security.

Users of all University information, including information classified as restricted, or information which carries additional obligations (such as those relating to confidentiality), must ensure they are aware of their individual responsibilities for complying with University and departmental policies on information security, as well as legislative requirements.

4.7 Third parties

All agreements and contractual arrangements with third parties which include accessing, processing, communicating or managing the University's information, or information systems, should cover all relevant security requirements, including compliance with this policy. The University's privacy notices must be consulted in cases where personal data is agreed to be shared with third parties; if in any doubt about the lawfulness of such sharing, the risks of these activities must be assessed, and the Data Protection Officer consulted.

5. Integrity and availability of information

5.1 Integrity of information

Integrity refers to the accuracy, consistency and completeness of information across its life cycle. Accurate information supports good decision making. For personal data, ensuring data accuracy is a legal requirement.

Loss of integrity can occur at any stage in the lifecycle of information, particularly when it is being updated, transferred or stored. Training and support for those handling information, and an awareness of the need for accuracy, are as important as technological checks or validation methods for maintaining integrity. It is the responsibility of those using data to check that care is taken to ensure that errors are not introduced at any stage.

The integrity of electronic data can also be compromised through viruses, malware, hacking, and other cyber threats, as well as through hardware errors, such as hard disk or memory device failure. Information systems will be protected by appropriate virus-check software, firewalls, and other mechanisms, and through both essential and ad hoc user training to help individuals identify and deal with viruses, phishing, and other attacks.

The integrity of paper information can be compromised through poor quality copying, inaccurate labelling, inadequate version control, poor filing practice, and/or poor storage methods.

5.2 Availability of information

Timely access supports efficient working, good decision making and service delivery. Availability is about more than just remote access: it includes paper items being clearly labelled and promptly and correctly filed to aid speedy retrieval.

Digital Innovation and Technology Services, and others providing systems, software or services, must ensure that systems are robust, backed-up, and that business continuity arrangements are in place, and available to be implemented as required.

Individuals also hold responsibility for the availability of information over which they have control, including ensuring that information that needs to be shared is available to those who need to have access to it, while respecting the principles of data minimisation.

Access to email and all other University systems will cease immediately after an individual's last day of employment.

5.3 Use of mobile devices

This policy covers information and information systems however accessed, including when accessed on mobile devices, regardless of whether those devices are personally owned or issued by or through the University. Adequate protection for mobile devices and the information stored on or accessed through them should be in place, including encryption, where appropriate.

Use of mobile devices must comply with specific policies for their use as well as with the more general polices on use of IT.

5.4 Use of Third Party Cloud Services

Cloud-based file hosting services[2] are third parties and therefore the user has no direct control over the management and security of data that is entrusted to them. When using such services individuals must seek assurance through due diligence and contractual obligations, whilst ensuring compliance with UK law and applicable regulations. Risk factors to be considered are that data are being entrusted to a third party, can be accessed by anyone connected to the internet if they provide the right credentials and may cross international boundaries and legislative regimes. Whilst it may be possible to transfer commercial or financial risk, the information risk always remains with the University. Before using cloud services consideration must be given to whether the cloud service is secure enough for this type of information, whether it is compliant, and will remain compliant, with relevant legislation, contractual or regulatory requirements and whether any other risks that arise from using this service are acceptable. It should also be borne in mind that information processed using cloud services may be required, legally, to be disclosed under the Freedom of Information Act 2000, and/or as part of data subject access requests. As data held by these cloud-based file hosting services are not backed up by the University, the responsibility for backing up rests with the user. When using a third-party cloud service in connection with their University work, users should log in using their University of Essex email address

[2] Examples of such services include Dropbox or Google Drive; other services exist.

along with a unique strong password, which should be different from their University password. Users should ensure that any work-related data are kept separate from any personal data by not mixing data in the same account and accessing their work account using their University email address, only storing work data in that account.

5.4 Incident reporting

Any loss of integrity or availability should be reported to the relevant system owner.

5.5 Purchase of information systems and software

All IT and information-related software, systems and hardware must be purchased in line with procurement legislation. The contractual agreements relating to such purchases must also comply with data protection legislation. Digital Innovation and Technology Services and Procurement should be made aware of any potential purchases of IT and information-related software, systems and hardware. The Data Protection Officer should be consulted at an early stage in consideration of any purchase to identify whether the completion of a Data Protection Impact Assessment is required.

6. Personal data

Personal data must be handled in accordance with the Data Protection Act 2018 (DPA), and the UK General Data Protection Regulations (UK GDPR) and related UK legislation, and in accordance with the University's policies and guidance on personal data.

A higher level of security should be provided for sensitive personal data, defined in the DPA as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences. This higher level of security will apply also to the special categories of personal data, which are defined in UK GDPR as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, the genetic data, biometric data processed solely to uniquely identify an individual, and data concerning health, sex life or sexual orientation.

7. Protection of restricted information

A case-by-case approach must be taken to identify whether information needs to be restricted, with due regard given to the University's obligations to academic freedom and freedom of speech.

Information may be restricted if to do so would be within the law, and the information in question is confidential by nature, has been provided on the understanding that it is confidential, and/or its loss or unauthorised disclosure could have, for example, one or more of the following non-exhaustive consequences:

- financial loss, e.g., the withdrawal of a research grant or donation, a fine by a regulatory body, a legal claim for breach of confidence, disclosure of commercially confidential information compromising competitiveness
- non-compliance with the terms and conditions of an agreement or contract, and/or
- an adverse effect on the safety or well-being of members of the University or those associated with it

This is not an exhaustive list and other reasons, particular to the information in question, may require it to be restricted in circulation, if to do so would be lawful.

This policy position does not undermine the University's fulfilment of its duties as a higher education institution with reference to academic and freedom of speech. We are a University that values academic freedom and freedom of speech within the law.[3] We see these as vital components of being an inclusive community. Academic Freedom is an essential part of academic and University life and flourishes where there is tolerance of a wide range of views and beliefs which are lawfully expressed. Promoting the lawful expression of diverse views on our campuses and through events that we hold, including the lawful expression of views that some may find objectionable or offensive, is an important part of our responsibility to be inclusive. It enables all members of the University to feel able to express their views and beliefs within the law and encouraged to be active members of our University community.

Similarly, this policy position does not undermine the University's fulfilment of its obligations as a public authority under the Freedom of Information Act 2000 (FOIA). The University will ensure that information which it is required, by law, to disclose, and to which exemptions do not apply, will be made available in response to requests under FOIA.

7.1 Storage

Some sections or departments, depending on the nature of the information used, are required to implement additional controls, such as clear desk policies or data encryption in order to provide adequate protection for personal or restricted data.

[3] https://www.essex.ac.uk/about/academic-freedom-and-freedom-of-speech

Restricted information should be kept secure, using, where practicable, dedicated systems storage (such as Box) rather than local storage (e.g., a PC hard disk), with an appropriate level of physical security. Hard copies of restricted or sensitive information must always be kept in locked physical units.

Data encryption should be considered as an additional security layer, where physical security is considered insufficient for electronic information. This is particularly relevant for information stored on or accessed through mobile devices.

7.2 Access

Restricted information must be stored in such a way as to ensure that only those authorised to do so can access it.

All users must be authenticated. Authentication should be appropriate, and, where passwords are used, clearly defined policies should be in place and implemented. Users must follow good security practices in the selection and use of passwords.

Additional forms of authentication will be considered as appropriate on a risk assessed basis.

Where needed, access records will be kept as appropriate for each system or operation, or as required by relevant regulation or legislation.

Physical access should be monitored, and access records maintained, which could be via audit trails, logbooks, CCTV, etc as required.

7.3 Access control

Access to restricted information must be controlled via well-defined access control arrangements which allow the appropriate level of access, with this level being reviewed and approved by a senior member of staff in each area of work. Levels of access control should be reviewed at least annually and always when an individual changes role.

Any access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.

Restricted information in hard copy, whether already existing in that form, or printed from electronic sources, must be kept securely at all times if it needs to be removed from University premises.

7.4 Copying

The number of copies made of restricted information, whether on portable devices or media, or in hard copy, should be the minimum required to meet the purpose, and, where necessary, a record kept of their distribution. In general, providing access to a single version is preferred to the creation and distribution of copies.

All copies should be treated with at least the same security considerations as the original, for example, by using encryption and physical security (e.g. stored in a locked cupboard, drawer or filing cabinet). When no longer needed, copies should be deleted or, in the case of hard copies, securely destroyed.

7.5 Disposal

Policies and procedures for the secure disposal or destruction of restricted information must be followed.

7.6 Transfer and sharing of information including email

Human error underlies the majority of inappropriate sharing of information at the University. Before sharing information through any channel or medium, individuals must check whether or not the information is restricted. If the information is restricted or sensitive in any way individuals must ensure that the channel they are using offers an adequate level of protection and that the information is properly directed, by double checking email addresses, mailing labels, etc.

Senders of email must ensure that all recipients, including those on the CC or BCC list, are entitled to have the information shared with them, and that restricted information is not accidentally shared via long email trails.

Due to the confidential nature of University committee papers these must only be shared via Box, the University's approved file sharing system, by uploading papers to the relevant Box folders set up by the Governance Team. Sharing information in this way is far more secure than sharing files via email.

7.6 System Planning and Acceptance

A risk assessment should be carried out as part of the business case for any new information system that may be used to store restricted information. The risk assessment should be reviewed periodically on existing systems. A Data Protection Impact Assessment (DPIA) should also be carried out where appropriate.

7.7 Resilience

Information must be handled and stored in such a way that its confidentiality, integrity and availability are safeguarded, to mitigate the risks of loss or unauthorised disclosure, and to preserve business continuity. Information and information systems, including hardware, should have appropriate levels of resilience. Information owners should determine, as part of their risk assessments, whether higher levels of resilience than those centrally provided are required.

7.8 Enforcement

The University has established this policy to promote information security within the organisation, and to ensure compliance with the University's statutory obligations. Any failure to comply with this policy may result in appropriate disciplinary procedures being followed.

Any loss or unauthorised disclosure of information in any form must be promptly notified to the Data Protection Officer, in line with the University's Data Breach Response Policy. Notification should take place as soon as possible and within one hour at the maximum of such a disclosure coming to the attention of a member of staff. The Data Protection Officer will ensure that the incident is investigated, will advise on remedial action to be taken promptly, and will ensure that it is reported as necessary. If in any doubt, the Data Protection Officer must be contacted. Reporting may be required to the relevant group or committee, Head of Department or Section, Registrar and Secretary, Vice Chancellor, Council and to relevant external authorities (for example the Information Commissioner's Office).

8. Other relevant University policies and guidance

- IT Acceptable Use Policy (Essex users only)
- IT Acceptable Use Policy Guidance (Essex users only)
- Data Protection Policy (.pdf)
- University Third Party Contact Policy: sharing registered students' information (.docx)
- Guidelines for Using Your Personal Device for Work or Study
- Data Breach Response Policy (Essex users only) (.pdf)
- Data Protection Impact Assessment Policy (.pdf)

Policy Information

Field	Description
Title	Data Protection Policy
Policy Classification	Policy
Security Classification	Open
Policy Manager Role	Data Protection Officer
Responsible UoE Section	Office of the Vice Chancellor
Publication Status	Published
Published Date	5 December 2024
Last Review Date	November 2024
Minimum Review Frequency	Annual
Review Date	December 2025
UoE Identifier	0214

If you require this document in an alternative format, such as braille, please contact the nominated contact at dpo@essex.ac.uk.