Electronic Information Security Policy

Contents

Page left blank for printing

1 The University's Electronic Information Security Policy

In order to use the University's IT systems and services, all 'users' (students, staff and visitors) are required to comply with the following code of conduct:

a) This policy applies to the use of any University IT facility, *including* for example the use of a personally owned device that is attached to the University's wifi or to any other University IT asset or service.

b) All users are required to report any misuse of IT systems, any infringement of this policy and any issue that may endanger full compliance with relevant UK Data Protection legislation.

c) All *private*[1] and *confidential*[1] information (electronic and paper), and the means of accessing it (using a PC/Laptop/ Smartphone) should be physically secured (locked away) when not being used.

d) You must inform the University if you believe there may be any risk of breach or potential breach of UK Data Protection legislation through information loss, or of any unauthorised access to information.

e) You must report the loss of any computing equipment that might contain confidential[1] information.

f) Users should not intentionally cause damage, access or alter admin device or systems settings, or otherwise jeopardise the integrity of computer equipment, software or network services.

g) Anti-virus software must be used on any personal equipment used to access University services.

h) Users must abide by all agreements and contracts by which software and any associated information are accessed using University computing services. Specifically, users must not install, replace or update information on University computing equipment without appropriate authority[2].

i) Users must not alter or install unauthorised software onto University computing equipment without appropriate authority[2].

j) Users must not take University IT equipment off-campus, without the appropriate authority[2] to do so.

k) Users must not use any University computing services to gain unauthorised access to any other computing system (internal or external). This includes any unauthorised access to any other person or organisation's computer systems or data, or any other copyrighted material[3].

l) You must not acquire or distribute *unauthorised*[1] information, and you must not use University IT systems or services for acquiring, storing, receiving or transmitting offensive, indecent or obscene material. This includes through web browsing, where using proxy-avoidance and anonymiser websites is expressly prohibited[4].

m) Information should be stored in the most suitable facility, for example if a case management system exists, related confidential information should not be stored in ad-hoc general storage such as network drives, cloud or removable media such USB Sticks.

n) Users must avoid sharing any documents or folders made available to them, particularly if these contain any private[1] or confidential[1] information.

o) Users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening[5], discriminatory or extremist. The University observes the Prevent Duty of Care and reserves the right to block or monitor access to such material

p) Users must not use University IT systems or services for any commercial activity[6] without appropriate authority[2] from IT Services or their Head of Department.

q) Users are not permitted to use University IT systems and services for private commercial purposes or any other employment outside the scope of that person's official duties or functions.

r) IT Disposal – users must return any University owned IT equipment to IT Services for secure disposal.

The Code of Conduct is an integral element of the Electronic Information Security Policy, and the University's Acceptable IT use policy – please http://help.chi.ac.uk/it-strategy-and-policies

[1] For definitions of Private, Confidential and Unauthorised information please see the Electronic Information Security Policy
[2] *Appropriate authority* means, formal agreement from a relevant Head of Department and IT, recorded through the SIZ support desk.
[3] This particularly includes downloading copies of films and music outside of their copyright requirements.
[4] Exceptions can be made for the collection and storage of sensitive materials for authorised research
[5] This includes anything that might be considered as bullying, harassment or stalking
[6] This is because University equipment uses discounted HE software licensing, and commercial licenses may be required.

Page left blank for printing

2 Background and Purpose of the Electronic Information Security Policy

Electronic information is increasingly essential to all aspects of the function of the University. The loss or exposure of some information may only be inconvenient. However, exposure of other information may have significant consequences, particularly if it is personal information that relates to an individual or to individuals.

It is fundamental to UK data Protection Legislation to not retain information unnecessarily, beyond when anyone involved might expect, and of course the more information that is held, the greater the risk of inaccuracy, and or of this data being seen by someone unauthorised to do so.

UK Data Protection Legislation incorporates for example the Data Protection Act (**DPA**) and the General Data Protection Rules (**GDPR**) which aim to protect every individual's right to privacy. These legislate that information created and held by an organisation is; held securely, used only for the purpose for which it is intended, and is not retained for longer than that purpose required. This document focuses on the principle of 'held securely'.

! The University has to achieve legitimate access to information (for its intended purpose) *and* security from unauthorised access. This is particularly and specifically the case when dealing with personal information

The consequences of the; misuse, unauthorised access to, or the loss of someone's personal information are significant ethically, reputationally *and* legally. If there is any negligence (however unintentional), the UK Government's Information Commissioner's Office (ICO) can fine an organisation up to 4% of its annual turn-over, over and above the (unlimited) damages that can be awarded by a court to any one or all of the people affected.

! Avoiding the loss or unauthorised access to information can only be partly met by technological safeguards, compliance also requires awareness and actions by the people who acquire, create and store information.

2.1 Purpose of this document

The security policy is set out in Section 1. This policy sets out the principles you must abide by when using any University systems or infrastructure or where your activity is related to the University, even if this is just to use a University email address to undertake some personal business. The policy applies to students, staff and visitors and is needed to ensure the University meets its statutory responsibilities to data protection.

This document and the policy is complementary to the training and support for awareness of Data Protection. For a fuller understanding of Data Protection, please undertake the on-line training available at; https://moodle.chi.ac.uk/course/view.php?id=80951 Further training on the principles of cyber security can also be accessed through the on-line tools at http://moodle.chi.ac.uk/course/view.php?id=71953

There is further information on how to stay safe on line, available at: http://help.chi.ac.uk/students/security

The remainder of this document sets out the background and mechanisms through which all students, staff and visitors can minimise the risks of the exposure of other people's personal information.

2.2 Background to the need for an Electronic Information Security Policy

Technology is an enabler to creating, storing ad accessing information, and the University applies the 'best of breed' technical facilities and services in the physical and logical safeguards used across the University (encryption, passwords and anti-hacking measures).

This policy focuses on electronically held information, but it should be noted that Data Protection principles, equally requires there to be avoidance of the unauthorised access to, and the loss of paper-based information. The University undertakes regular internal and external audits and reviews and can (at any time) be subjected to a review by the UK Government's Information Commissioner's Office.

Minimising risks requires the active participation of all University stakeholders (all students, staff, visitors and suppliers) that have access to create, acquire or access information, and particularly where that information involves the *confidential* details of other people, or information which would otherwise be considered *private*.

2.3 Review and update of the policy

The policy set out in Section 1 is reviewed at least annually, or more regularly if new threats emerge.

Page left blank for printing

3 Categorising the sensitivity of information

In the context of the University, there are four main classes of information which may affect some or all students, staff and visitors and partners;

Category A - Public
Any data / information that can appropriately be viewed by anyone, anywhere e.g. press releases, course information, publications, released research data, conference papers etc.

Category B - Private
Private information is data / information which is intended to be limited to specified members of the University of Chichester on a need to know basis e.g. reports, financial plans, guidance, collaborative documents, draft documents, teaching materials etc. Private may also include information bound by copyright, or which relates to the performance rights or intellectual property of its originator.

Category C - Confidential (Sensitive personal Information)
Confidential information is that which relates to a living individual, and who can be identified from that information. Data Protection legislation typically focuses on where you (individually and / or as an organisation) have a copy of information relating to another person. This can be any data which identifies an individual, opinions about an individual or photographs of them. This data relating to other people requires the strongest possible technical and physical safeguards and clearly defined processes to ensure it cannot be seen by anyone not authorised to do so. Examples of personal confidential data include;

- Name, date of birth, address, phone number, email address
- Racial or ethnic origin.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Trade union membership.
- Genetic
- Biometric information (eg. where used for ID purposes)
- Physical or mental health or condition.
- Sexual life or sexual orientation.

Any piece of information which contains any of the above is inherently confidential. This includes, a student's assessment (because it names them) is confidential[7].

Category D – Unauthorised
Any data/information which is personally owned, or which belongs to a 3rd party should not be downloaded to, stored on or distributed using University equipment and services, this includes.

- Data that is no longer required, whose time or original purpose has passed
- Information that would be better protected by being stored in a case management system[8]
- Personally owned music files, video files and photographs,
- Personally owned (whether free or licensed) software,
- University branded or owned information on (or linked from) Social media
- Any information created or stored on counterfeit equipment, or in unlicensed software
- Unregistered personal information (see Data Protection Act, 1998)
- Any information (incusing music and video) that is not compliant with University policies, procedures or current legislation, and any information being accessed, viewed or used consciously or unconsciously in any illegal act, including their copyright conditions and licencing.

Please note that there is no single, or universally agreed definition of the sensitivity of data/information. The categories above are indicative, and within the following guidance to correlate the sensitivity to the device and circumstances that information might be created and acquired. The terms *Data* and *Information* are often used interchangeably within Data Protection legislation and in the General Data Protection Regulations (GDPR).

[7] Further information is available at http://www.chi.ac.uk/about-us/about-us/how-we-work/policies/data-protection

[8] For example HR data, and photographs of staff or students and any other confidential information for which explicit consent has not been established, should not be retained in ad-hoc storage such as network drives, PC hard drives, USB sticks, mobile telephones. Such information should only be stored in case management systems.

Page left blank for printing

4 Information Security and Devices and Storage

For confidential information, a relevant case management system with its inherent access controls and data management facilities should be used wherever possible. Where this is not possible, (for example students research projects may name and even characterise participants) network storage is the most secure form of ad-hoc storage (This will need to be monitored for when the data should be removed).

4.1 Network Storage

Home drives: All students and staff have access to network storage known as their *home* drive or H: drive. This is secure network storage for personal University data is attached to their network account, which can be securely accessed from a computer or device connected to the Internet.

Shared drives: There are additional network storage facilities called shared drives or S: drive. This network storage is available to multiple users enabling collaboration and sharing.

Advantages of using Network Storage: The University's network storage can be used for all categories of information. This Data is protected by University information security systems, is routinely backed up for business continuity purposes as well as to enable the recovery of data that is accidentally deleted.

4.2 Portable Devices

University Issued Devices: Portable devices (such as laptops, tablets and smartphones) may be issued/loaned to enable access University resources whether at a desk, or on the move. Security measures are installed, and users are directed to store any data on their network storage.

Personal Devices: The University enables access to University systems and services through a staff, student or visitor's own device. Access is controlled through authentication to each system or service. Users also have a responsibility to ensure their devices are protected, e.g. use a boot password, a screen saver with a password, disk encryption and anti-virus software, even if you only ever access public data. You must not download private or confidential data to a personal device.

Working off campus: Please remember to exercise extra caution when connecting to 3rd party wireless networks (at home, in a coffee shop or hotel for example). Any WiFi which does not require authentication via a user ID and password should be regarded as risky and non-secure.

4.3 Portable Storage

University Issued Storage Media: Portable storage media (CDs/DVDs, USB drives and external hard drives) may be issued/loaned to members of the University. Security measures (such as encryption software) are used to help reduce the risks, however due to the potential of their being lost, portable storage media are not suitable for storing confidential information.

Personal Storage Media: The University does not currently restrict the use of personal storage media; however, their use for private and confidential University data is **not** permitted.

Mobile Telephones: Data on mobile phones cannot be backed-up. Mobile phones can be lost or stolen and have very little security. They must not be used to store private or confidential data

Considerations when using Portable Devices and/or Storage Media

- Files stored only on portable devices and/or storage media have no provision for backup or recovery if they become lost, stolen or corrupted.
- There is a significant risk of reputational damage and/or litigation and fines if data is stored inappropriately on portable devices, especially when it could have been stored in a case system or on network storage.
- If it cannot be avoided, any private and confidential data that *has* to be temporarily copied to University issued devices or storage media, these devices and media **must** be encrypted. Following such use, this media must be returned to SIZ for secure cleaning and disposal.
- Personal devices/storage media, including personal email accounts must **not** be used to store private and confidential data.

4.4 Cloud Storage

University Cloud Storage: All staff and students have access to the University's cloud storage – *OneDrive for Business*. One Drive for Business (ODFB) can be accessed on and off campus. ODFB should not be used for confidential data, (and networked H / S storage should be used).

Other Public Cloud Storage: Other commercial cloud providers, such as Dropbox, iCloud, Google etc. also offer public online storage. However, the service levels offered by these providers are beyond the control of the University and their use for University data is **not** permitted.

Considerations when using Cloud storage

- OneDrive for Business is protected by industry standard security systems and even files you delete are recoverable (for up to 90 days).
- Private and confidential data **must not** be uploaded to any personal cloud storage service
- Synchronisation between ODFB and non University devices **must** be turned off for all categories of data.

4.5 Email

University email: Staff and Students are provided with University email accounts. Many day-to-day activities are undertaken using email, e.g. meeting requests, documents, business decisions, and requests for service/information. Confidential data should not be sent or stored as an email, (and should be removed to a case management system as soon as possible).

Personal email: Many staff and students also have personal email through providers such as Gmail and Yahoo. The University permits users to access their personal email accounts on campus, however their use for private and for confidential data is **not** permitted.

Email on mobile telephones: Mobile phones (of all makes) have very little security. Email on a mobile phone increase the risks of unauthorised access to accounts data and passwords. With a mobile phone, only web-email can be used. Email passwords should not be set to be 'remembered' by the device, and email should not be downloaded to the device.

! Considerations when using email

- Be careful to ensure you have spelled the email address you are sending to, correctly, a misspelled email could mean information being sent to an unauthorised person.
- Email is an unsecured communication tool, what you send can easily be intercepted (and read).
- University email should only be used for temporary storage of any type of data. Email attachments, and any email containing private or confidential data should always be removed to network storage.
- Personal email must not be used to transmit or store private and confidential data in or out.
- Any confidential content you receive by email, can be removed to case system, and or network storage.
- Mobile phones should only use password protected web-based email. You should not use an email 'client' service that downloads email to the device.
- The University's email system will delete appointments, and sent mail that is more than 12 months old.
- There are lots of scam emails[9] sent to the University, please keep abreast of these by regularly looking at the University traffic lights http://help.chi.ac.uk/ and at the help pages http://help.chi.ac.uk/email-scam-and-virus-advice

! If you are unsure about how to categorise your data and where you can store your data please contact the Support and Information Zone (SIZ)

! If you think you may have received a scam email, see http://help.chi.ac.uk/reporting-suspicious-emails and / or contact the SIZ.

[9] Scams often try to get you to follow a link, and to enter your password (thus compromising it).

4.6 Summary view of methods of its storage.

Category[10]	Method																	
	University Systems[11]		University network		University SharePoint		Cloud Storage		Desktop & Laptop Computers		Mobile Phones		USB Sticks / Ext drives SD Cards / CDs		Secure Email		General Email		Social Media	
																				
	UoC	H:\ S:\	UoC	UoC	Your Own	UoC	Your Own	UoC	Your Own	UoC	Your Own	UoC	Your Own	UoC	Your Own	UoC	Your Own	UoC	Your Own
A Public	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
B Private	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	✓	✗	✗	✗
C Confidential	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
D Unauthorised	✗	✗	✗	✗	!	✗	!	✗	!	✗	!	✗	!	✗	!	✗	!	✗	!

✓ Approved storage method

✓ Approved storage method, only if a suitable corporate system is not available, but must have restricted access, and must have retention management.

✓ Approved storage method only if encrypted, and only temporarily until the data can be relocated to a corporate system

✗ Strictly prohibited

! This is outside of University responsibilities, but we would strongly counsel you to consider this carefully

[10] See definitions on page 5

[11] For example, the Tribal Students Record System (SITS), the ITrent Human Resource system etc,

4.7 Securing and taking care of your personal and University equipment

It is important to know where your devices are, and to keep them safe. This is because that (by far!), the most frequent method of unauthorised access to private and confidential information is through a fraudster stealing or otherwise accessing a PC, Tablet, or Smartphone. For any device (whether owned by the University or not) that can access University information, you should ensure that you have up to date virus protection, hard-disk encryption, screen-locks that are actioned when the device is not in use,

! It is far more secure to fully close down a PC/Laptop/Tablet, than to leave it in 'sleep' mode.

Smartphones (of all manufacturers) are particularly vulnerable to theft and loss, and also have much weaker security than (for example) a Laptop. It is important to have a screen lock, and to keep the phone safe. Fingerprint and face recognition are improving but still leave smartphones vulnerable.

If you believe the phone to be lost or stolen, you should contact SIZ immediately. You can use the in-built utilities to locate your phone, and if necessary to send a 'self-destruct' instruction to your phone, which can wipe all data and apps from it, locate the phone, or make the phone inoperable. Help in how to do this can be found at:

Android Phones: https://support.google.com/accounts/answer/6160491?hl=en&ref_topic=7189042

Apple Phones: https://support.apple.com/kb/PH2701?locale=en_GB

It is good practice to keep your computing equipment safe, and ideally locked away. As set out in the code of conduct, University devices are only provided for University business, and should not be taken to places that increase the risks of loss or theft.

! You should not leave University devices unattended, and it is particularly high risk to leave University, (or your own PC, Tablet, Smartphone) devices in a car.

4.8 What to do if your device has been; lost, stolen or accessed by someone else.

If you believe your device is lost or stolen, you should contact SIZ immediately. Similarly, if you believe your device may have been used by someone else, you should contact SIZ immediately.

! The University is statutorily required to notify the Office of the Information Commissioner of any suspected loss, within 72 hours (and can be fined for failing to do so)

SIZ will initiate the notification to the UK Government's office of the Information Commissioner and will commence the University's risk assessment to ensure that any risk of the device being used to access confidential information is minimised. SIZ may ask you to liaise with IT to assess whether the device has been used in such a way as to suggest that private or confidential information has been accessed, or if it has been used to access unauthorised information.

! University devices are provided for University business.

You should not use and University device for any unauthorised activity. You should avoid anyone else (including family members) using your University devices. As is set out in Section 6, please note that all internet browsing using University facilities and devices is logged, 24 hours per day, and wherever it is used (including for example from home).

5 Information Security, for Identifiers and Passwords

Access to information comprises of regulated access to the University's infrastructure (internet for example) and devices (printers for example) , and then on a user by user, case by case basis to each of the University's business systems (Moodle, SITS etc.). Each University device has single sign on, to all systems and services. For personal devices, the password for access to University Systems and Services has to be entered manually after the device has been started, inclusive of any personal, local passwords this might entail.

! The named account holder is accountable for all use of the ID and passwords for their University account.

5.1 Risks – Identifiers and Passwords

Having an Identifier (ID) and a password to the device (your Laptop for example), and to the location(s) the device can access, are mechanisms that aim to protect both your own information, and to assist you in protecting other people's information. The approach you take to your identifier(s), and your passwords are significant to the risks of someone else finding these out, and impersonating (spoofing) you.

Having a different ID and password for the device (Laptop for example), and for the locations (Cloud Storage) and different ID/Password for access to each system reduces risks, however this approach is seen as being inconvenient and unpopular. Consequently, it is important to realise that your 'single-sign-on' IDs and Passwords can if 'harvested' be used on other equipment, to get further and deeper unauthorised access.

! However convenient it might be, it is unwise to use the same ID and Password you use in social media, in your University accounts, or in your on-line banking etc.

In any case, keeping your ID and Passwords secret is absolutely essential. Allowing your device to remember your passwords (caching) is extremely high risk, a risk that is exponentially increased if you do not set a device password (Also known as a boot password) that prevents the device being switched on without a password. Please note that the locations in which devices store the 'caches' of your individual and single-sign-on passwords are the prime target of hackers, and your device may be targeted for mugging or theft.

! Stealing your device in the hope of finding your stored passwords is primarily what thieves are after

Over 2000 smartphones and about 1500 laptops are stolen every day in the UK, and it is the potential access to ID and password information that is of most value to most criminals, not the resale value of a secondhand IT.

Provided you report it, IT can disable your single-sign-on and the individual passwords that give access to network storage, and corporate systems.

! NB the more systems you have access to, the higher your risks and the greater your responsibilities

Access for devices attached to the University's network and systems is monitored, and access is suspended where there has been inactivity for more than 5 minutes. The systems that contain more sensitive information may require that you re-enter your password after a period of inactivity to reduce the risks of an opportunist individual finding an unattended device, and therefore having access to everything *you* have access to.

5.2 Password Hygiene

All users must manage the password associated with their identifiers for each service they are authorised to access in a safe and secure manner. It is good practice that;

- Each password is appropriate and secret
- Passwords should not be guessable i.e. not! your partner's name, dates of birth, or names of your children
- Passwords or logon details should never be divulged to **any** person; this includes the account holder's manager, colleagues, staff and members of SIZ or IT Services
- Identifiers, Passwords and logon details should **not** be written down
- Do not be fooled by scams that entice you to follow a link, and enter your password into their scam site.

- You should not let your web-browser remember (*cache*) your passwords
- You should not use your University ID and Password for access to any other website or service

To facilitate the secure management of passwords on the IT systems, the following rules are applied:

- It is good practice to change passwords regularly, recommendations from the Information Commissioner's Office, and under ISO27001 vary in advising this is done between every 15 to every 60 days.
- Passwords for the main University network will automatically **expire after one year for staff and after the completion of a student's course**; passwords may not be reused.
- Passwords require a minimum of EIGHT characters (one of which must be numeric) with a mixture of upper and lower case characters. A stronger password will include at least one symbol (+, -, *, #, etc).
- Requests for password resets can be made via the FastPass self-service facility available (24 hours a day, 7 days a week) via the University Internet site or alternatively can be handled by the SIZ.

! **Help and advice is available from the Support and Information Zone 01243 816222, help@chi.ac.uk and general guidance is published on the IT Help web pages http://help.chi.ac.uk/ .**

6 Information Security and University Monitoring

In addition to our own commitments to privacy and confidentiality, the University is legally obliged to ensure that computing services (hardware, software, network services) are used appropriately in support of institutional activities and to ensure compliance with statutory provisions and licence agreements.

The University's IT Systems and services are provided to enable staff, students and guests to carry out their work, research or studies. On activating an IT account at the University, the user is explicitly bound by this Policy.

Initial awareness of the policy is incorporated into induction training for staff and students. For any member of staff who is inviting a partner, or a visiting academic to the University, they should advise the partner / visitor to review this policy. Incidents and questions logged with SIZ, and the incidence of access to this document is logged as a relative measure of the levels of awareness, to inform additional guidance and advice.

6.1 Monitoring the awareness and compliance with the policy

The policy is made available to students, and to staff. Staff awareness of the policy is assisted by inclusion in the induction process and is refreshed annually, or more frequently if new threats or new practices emerge.

The policy is referenced in the log-in process of all University owned PCs and Laptops. This include that the user may review it beforehand but is inherently bound by the policy if they log into the device.

6.2 Managing Social Media

University social media is a useful mechanism for communicating public information. Although some social media can allow for closed, members only groups, Social media is not suitable for storing, or communicating private or confidential information.

! **The social media policy can be accessed here** http://help.chi.ac.uk/strategy-and-policies

Personal social media is discussed in the policy, however it is important to note that your work, and non work identities are often intertwined, and as such what is non work, can become associated with the University.

6.3 Monitoring IT and telehony systems

In order to ensure the University's compliance with UK Data Protection Legislation, (for example the Data Protection Act and General Data Protection Regulations - GDPR), use of the University's IT Systems, telephony and infrastructure may be subject to monitoring and logging.

Accessing internet sites (using the University's IT services, including those accessed from off-campus) is **routinely** logged. Accessing certain classifications of internet sites or making calls to certain types of telephony services is prohibited (copyright infringement, threat of violence, known sources of extremism etc). All attempts to access these types of sites or services are logged and can be evaluated for safeguarding and / or investigation. Where you need access for legitimate, approved research these can be un-prohibited for named individuals, for fixed periods of time.

Only in exceptional circumstances are the logs of websites a user has visited assessed, and this follows the same process for if there is a need to access a user's stored information. Exceptional circumstances include where;

- A request is made by the security forces
- There are concerns that the user of the It is at the risk of radicalism
- A request is made by a police force investigating alleged criminal activity, or in support of other law enforcement processes
- The University is undertaking an internal investigation in line with its published Policies and Procedures
- The University is required to provide information to external bodies such as a software licensing company in line with the terms and conditions of a licensing agreement
- The Vice Chancellors Group (VCG) determines that monitoring or investigation is necessary to ensure compliance with the law or with University Policies and Procedures.

6.4 Reporting

All incidents where there is any risk of information loss, or unauthorised access should be reported to SIZ. SIZ will liaise with the key IT and senior staff (For example the University Registrar, who is responsible for the University's DPA policy, and who is the liaison with the Information Commissioner's Office (ICO), to assess the level of risk.

Where there is a risk of the loss of information, the incident will be referred to the University' Serious Incident Management Team (SIMT).

6.5 The penalties for inadequate management of information

! You as well as the University can be prosecuted under UK Data Protection legislation

Penalties under UK Data Protection Legislation can be applied if the organisation is unable to prove that a device has not been lost (even temporarily), or if the University is unable to prove that unauthorised access has not taken place.

Whether or not there is ever any direct link of any criminal activity, unlimited compensation can be awarded to the individuals affected by information 'loss'. In addition, the Director Public Prosecutions, instructed by the UK Government's Information Commissioner can apply fines of up to 4% of the organisational annual turn-over, or £20m per incident, over and above any personal damages awarded.

The Information Commissioner's Office can also serve compliance orders, which might include appointing external experts (at further cost to the University) until they can ensure that the policies, awareness, technical and people procedures are secure.

! Please note: ignorance of the law, or transgressing law in ignorance is no defense

6.6 Consequences of non compliance with this policy

This policy is a guide and not an exhaustive list of what you should or should not do, and you should satisfy yourself of the best practices and the principles of law, a selection of which is listed in Appendix 1.

Any suspected failure to apply reasonable care, and any suspected infringement of the policy or any related legal requirements may result in the user's access being summarily withdrawn pending appropriate investigation, and

- action under the Disciplinary Policy and Procedure (for staff)
- action under the Academic Regulations (for students).

! in extreme circumstances any investigation into information loss may lead to civil or criminal proceedings for the University, and this may also be jointly or severally undertaken with you

7 Archiving and data disposal

All of the University's systems are secured using the latest and best methods and technologies. This policy seeks to avoid unauthorised access, but the legislation also expects that organisations should not unnecessarily acquire, or retain confidential data.

7.1 University Systems

The most secure location for confidential information is a case management system (for example the University's Student Information System, or HR Systems). These have specifically designed and approved access controls, and with agreed data management (retention / disposal) mechanisms. Where possible any ad-hoc confidential data should be transferred to and stored in a case management system.

! Please contact SIZ if you need help in copying confidential information to a case management system

7.2 Email and Instant Messaging Folders

In order to reduce the risks of data being compromised through unauthorised access, or overly long retention, certain folders in the University's email and instant messaging systems are automatically deleted each August.

- **Automatic, annual deletion of "Deleted Items".** When you delete an email from your inbox this is actually just removed into your Deleted Items folder. Any items older than 12 months in the Deleted Items folder will be automatically deleted each August.
- **Automatic, annual deletion of historic "Sent Items" and Calendar appointments.** Copies of sent emails, and of past calendar appointments that are than 24 months old will be automatically deleted each August.
- **Automatic, annual deletion of historic "Instant Messages".** Instant messages you sent and receive using the University's Skype, are recorded in your email account, in an email folder called 'Conversation History'. Any items older than 12 months in the Conversation History folder will be automatically deleted each August.

For anything that must be kept for a longer period, these can be transferred to a case management system (student record for example) to a different folder, and or to your H:\ storage.

! Please contact SIZ if you need help in deleting emails diary appointments or messages more frequently, and if you need help in transferring a confidential email to a more suitable storage facility

7.3 Leaving the University

On leaving the University your access to systems and services is ceased. Your University storage areas and email account are archived for between 30 and 90 days before being permanently deleted.

Where there is agreement to do so (and so long as it does not contravene UK Data Protection Legislation) copies of University private and public data (for example teaching notes, or your own research) may be made available for you to transfer to another organisation, or to a home account.

Students that leave the University can have their University email account and their University Cloud Storage, transferred to an Alumni account. (This is reversible if the Student returns for post-grad study etc). Alumni accounts are provided by Microsoft and are not managed by the University.

! Please contact SIZ if you need help in copying private and public data (whether you are staff of student)

Appendix 1: Summary of the main legal frameworks

This policy is a high level summary of the practices expected of any organisation, and its members. The policy is not exhaustive, nor does it over-ride statutory requirements. Use of University information and IT systems is subject to all relevant legislation, licence agreements, University Policies and other regulatory requirements which include the latest versions of, but are not limited to:

- Data Protection Act 1998
- The Protection from Harassment Act 1997
- Section 76 of the Serious Crime Act 2015 (Controlling or coercive behaviour)
- ss28-32 of the Crime and Disorder Act 1998 (CDA), (Harassment and Stalking)
- Stirring up racial or religious hatred under Part III of the Public Order Act 1986, in particular: publishing / distributing written material, and distributing / showing / playing a recording of visual images or sounds
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Protection of Children Act 1978
- Freedom of Information Act 2000
- Digital Economic Act 2010
- Malicious Communication Act 1988
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- The University of Chichester Social Media Policy http://help.chi.ac.uk/strategy-and-policies
- The Prevent Duty of Care (identification of vulnerability to extremism)
- Discrimination: https://www.gov.uk/discrimination-your-rights/types-of-discrimination
- Copyright Designs and Patents Act 1988
- Criminal Justice and Public Order Act 1994
- Chest Code of Conduct (See http://www.eduserv.org.uk/services/Chest-Agreements)
- Educational Recording Agency Licence
- Employment Code of Practice 2002
- General Data Protection Rules 2018
- Human Rights Act 1998
- Intellectual Property https://www.gov.uk/government/organisations/intellectual-property-office
- JANET Acceptable Use Policy (**J**oint **A**cademic **NET**work)
- Police and Criminal Evidence Act 1984
- Police and Justice Act 2006
- Marketing and Communications Policy
- Newspaper Licensing Agency Licence
- Obscene Publication Acts 1959 and 1964
- Obscenity: http://www.cps.gov.uk/legal/l_to_o/obscene_publications/
- Software Licence Agreements
- The Prevent Duty of Care (see https://www.gov.uk/government/publications/prevent-duty-guidance)
- WEEE Directive (Waste Electrical and Electronic Equipment Directive)

! Please note: It is the responsibility of each individual staff member, student or other stakeholder associated with the University to ensure they fully comply with the relevant and most up to date versions of legislation and any other regulatory requirements.

! The University's policy should be used as a guide to good practices, and not an exhaustive or authoritative statement of what you should do to comply with any relevant legislation.

! Please Remember: in accordance with UK Data Protection legislation and GDPR, you as well as the University are jointly and severally liable for your actions and their consequences; these could endanger our students, staff and partners, and can include both financial and reputational damage to the University.