|  |  |  |
| --- | --- | --- |
| Version number: | 2021 |  |
| Policy owner: | Dr R Matthews |
| Effective date: | 25/08/2021 |
| Review date: | 24/08/2023 |

Electronic Information Security Policy

#### Policy Statement

##### It is the policy of the University of Chichester (“University”) to ensure that electronic information is acquired and created all the time and is increasingly essential to all aspects of the function of the University.

##### Whilst the loss or exposure of some information would perhaps be no more than inconvenient, the loss or exposure of more sensitive could be extremely detrimental, particularly if it is personal information that relates to an individual or to individuals.

#####  The security of electronic information is therefore of paramount importance and something that all users of IT facilities provided by, or made available by, the University must share responsibility for, and ownership of, in order to successfully manage the potential risks involved. All users are required to accept this policy at the point of logging in

##### The purpose of this policy is:

###### to minimise the risks to the University arising from loss or exposure of information,

###### to raise awareness of the potential risks involved,

###### to provide all users with a clear articulation in the form of the Code of Conduct which follows below, of the University’s expectations regarding the use of IT facilities provided or made available, and;

###### to ensure consistency in the way IT facilities provided or made available are used.

## **Electronic Information Security Policy**

The code of conduct set out below, applies to all usage of IT facilities provided by, or made available by the University. This includes University IT equipment and services, but also covers any device (including personal devices) that uses the University’s WiFi or connects to any other University IT asset or service (for example, during remote working).

All ‘users’ (students, staff and visitors) of University’s IT systems and services are required to comply with this code of conduct. Failure to do so may result in access being withdrawn, and in serious cases, action under the applicable disciplinary policies.

**You must;**

* Use University IT systems and services for University business and in accordance with all University policies.
* Ensure that your use of University IT systems and services is appropriate, safe and in accordance with the purposes for which they are made available.
* Abide by all ‘terms of service’ and other contracts by which software and any associated information are accessed using University computing services.
* When using a personal device to access University IT systems or services, ensure that it is properly secured, for example by ensuring that your system is updated in line with manufacturer recommendations and that you have up-to-date anti-virus software installed.
* Report any misuse or abuse of IT systems, and any infringement of this code of conduct through the SIZ
* Store information in the most suitable (lowest risk) facility, for example in a University case management system or network folder, and not in ad-hoc or personal general storage such as cloud or removable media such USB Sticks.
* Secure (physically lock away) all private*[[1]](#footnote-1)* and confidential1 information (electronic and paper), and the means of accessing it (using a PC/Laptop/ Smartphone) when not being used.
* Inform the University [Director of IT] if you believe there has been a loss of private or confidential information, or a device (e.g., a laptop) containing such information.
* Inform the University’s Data Protection Officer immediately if you become aware of a loss of personal data, or a risk of such loss, or of any other credible and any issue that may endanger the University’s full compliance with UK Data Protection legislation.
* Advise SIZ of any leaving date, intermittence, or sabbatical to enable your access to services and information to be updated, and for you to return University owned IT

 **You must not;**

* Alter administrative device or systems settings, or otherwise jeopardise the integrity of computer equipment, software or information.
* Alter or install software onto University computing equipment[[2]](#footnote-2).
* Solicit, encourage or endorse use of, any non University or external computer system, or use a University system in a new context without first having consulted IT and the DPO and established whether a Data Protection Impact Assessment (DPIA) is required.
* Take University IT equipment off-campus, without the appropriate authority2 to do so.
* Use University IT systems or services for any non University activity2 without appropriate authority2 from IT Services and your Head of Department.
* Use your University identification or passwords with non University services.
* Use any University computing services to gain unauthorised access to any University or non-University information. This includes unauthorised access to copyrighted, personal, private or confidential material[[3]](#footnote-3).
* Acquire, store, share or distribute unauthorised1 information. This includes through web browsing, where using proxy-avoidance and anonymiser websites is expressly prohibited[[4]](#footnote-4).
* Create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening[[5]](#footnote-5), discriminatory or extremist[[6]](#footnote-6).
* Share any documents or folders you have access to, particularly any that contain private1 or confidential1 information, other than as required for University business and with the proper authorisation.
* Transform any confidential information communicated with you (for example using a recording of a video conference or copying any email or instant messages) to any other media or facility.

**!      Please review the privacy and use monitoring information and the guidance available on the help website (**[**link**](https://help.chi.ac.uk/privacy-and-monitoring)**)**

**!      Please review the Privacy Standard which is available on the University's main website (**[**link**](https://www.chi.ac.uk/about-us/policies-and-statements/data-protection)**)**

**!      Further information on how to use University IT, and to stay safe on-line is available on the help website - (**[**link**](https://help.chi.ac.uk/staying-safe-online)**)**

1. For definitions of Private, Confidential and Unauthorised information please see [(link)](https://help.chi.ac.uk/information-secure-storage) [↑](#footnote-ref-1)
2. This is because University equipment uses discounted HE software licensing, and commercial licenses may be required. [↑](#footnote-ref-2)
3. This particularly includes downloading copies of academic journals, films and music outside of their copyright requirements. [↑](#footnote-ref-3)
4. Exceptions can be made for the collection and storage of sensitive materials for authorised research  [↑](#footnote-ref-4)
5. This includes anything that might be considered as bullying, grooming, radicalisation, harassment or stalking [↑](#footnote-ref-5)
6. The University observes the Prevent Duty of Care  [Link to Prevent](https://www.gov.uk/government/publications/prevent-duty-guidance)  and reserves the right to block or monitor access to extremist material. [↑](#footnote-ref-6)