University of Brighton
Information Services

UoB IT Regulations

Last updated
By Q North
24th April 2018

Quick Guide

The following is a very brief summary of the main points of the University of Brighton Information Systems Regulations. You are expected to be familiar with the full regulations, which are available at https://www.brighton.ac.uk/is

- **Governance** Don't break the law, do abide by the University of Brighton's regulations and policies, and do observe the regulations of any third parties whose facilities you access.
- **Identity** Don't allow anyone else to use your IT credentials, don't disguise your online identity and don't attempt to obtain or use anyone else's.
- **Infrastructure** Don't put the institution's IT facilities at risk by introducing malware, interfering with hardware or loading unauthorised software.
- **Information** Safeguard personal data, respect other people's information and don't abuse copyright material. Remember that mobile devices may not be a secure way to handle information.
- **Behaviour** Don't waste IT resources, interfere with others' legitimate use or behave towards others in a way that would not be acceptable in the physical world.
- **Report** If you do see anything which you feel could lead to data being compromised, please do report it.

This document and other Information Services documents are held online on our website: https://staff.brighton.ac.uk/is

Contents

University of Brighton IT Regulations

1 Core regulations

The aim of these regulations is to help ensure that the University of Brighton's IT facilities can be used safely, lawfully and equitably.

The issues covered by these regulations are complex and you are strongly urged to read the accompanying guidance document, available at www.brighton.ac.uk/is. This gives more detailed information that we hope you will find useful.

1.1 Scope

These regulations apply to anyone using the IT facilities (hardware, software, data, network access, third party services, online services or *IT credentials*) provided or arranged by the University of Brighton.

1.2 Governance

When using IT, you remain subject to the same laws and regulations as in the physical world.

It is expected that your conduct is lawful. Furthermore, ignorance of the law is not considered to be an adequate defence for unlawful conduct.

When accessing services from another jurisdiction, you must abide by all relevant local laws, as well as those applicable to the location of the service.

You are bound by the University of Brighton's general regulations when using the IT facilities, available at www.brigfhton.ac.uk/is.

You must abide by the regulations applicable to any other organisation whose services you access such as Janet, Eduserv and Jisc Collections. When using services via eduroam, you are subject to both the regulations of the University of Brighton and the institution where you are accessing services.

Some software licences procured by the University of Brighton will set out obligations for the user – these should be adhered to. If you use any software or resources covered by a Chest agreement, you are deemed to have accepted the Eduserv User Acknowledgement of Third Party Rights. (See accompanying guidance for more detail.)

Breach of any applicable law or third party regulation will be regarded as a breach of these IT regulations

1.3 Authority

These regulations are issued under the authority of the Director of Information Services who is also responsible for their interpretation and enforcement, and who may also delegate such authority to other people.

You must not use the IT facilities without the permission of the Director of Information Services.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these regulations. If you feel that any such instructions are unreasonable or are not in support of these regulations, you may appeal to the Director of Information Services.

1.4 Intended Use

The IT facilities are provided for use in furtherance of the mission of the University of Brighton, for example to support a course of study, research or in connection with your employment by the institution.

Use of these facilities for personal activities (provided that it does not infringe any of the regulations and does not interfere with others' valid use) is permitted, but this is a privilege that may be withdrawn at any point. When using the facilities for personal activities be aware that in some circumstances your data may be provided to third parties as part of a legal obligation or as a result of other activity beyond the control of the University.

Use of these IT facilities for non-institutional commercial purposes or for personal gain requires the explicit approval of the Deputy Vice Chancellor.

Use of certain licences is only permitted for academic use and where applicable to the code of conduct published by the Combined Higher Education Software Team (CHEST). http://www.eduserv.ac.uk/services/Chest-Agreements See the accompanying guidance for further details. .

1.5 Identity

You must take all reasonable precautions to safeguard any *IT credentials* (for example a username and password, email address, smart card or other identity hardware) issued to you. You must not allow anyone else to use your IT credentials. No-one has the authority to ask you for your password, and you must not disclose it to anyone.

You must not attempt to obtain or use anyone else's credentials.

You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

1.6 Infrastructure

You must not do anything to jeopardise the integrity of the IT infrastructure by, for example, doing any of the following without approval:

- Damaging, reconfiguring or moving equipment;
- Loading software on the University of Brighton's equipment other than in approved circumstances;
- Reconfiguring or connecting equipment to the network other than by approved methods;
- Setting up servers or services on the network;
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent IT security measures.

1.7 Information

If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and must observe the University of Brighton's Data Protection and Information Security policies and guidance, available at www.brighton.ac.uk/is, particularly with regard to removable media, cloud services, mobile and privately owned devices.

You must not infringe copyright, or break the terms of licences for software or other material.

You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the University of Brighton's Data Protection officer.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory. The University of Brighton has procedures to approve and manage valid activities for research purposes that involve access to and/or storage of sensitive research material; these are available at https://staff.brighton.ac.uk/ease/ro/Pages/EthicsGov.aspx and must be observed.

You must abide by University of Brighton's external communications policies available from https://staff.brighton.ac.uk/mac/Pages/Communications.aspx when using the IT facilities to publish information.

1.8 Behaviour

Real world standards of behaviour apply online and on social networking platforms, such as Facebook, Blogger and Twitter.

You must not cause needless offence, concern or annoyance to others.

You should also adhere to the University of Brighton's guidelines on social media.

You must not send spam (unsolicited bulk email).

You must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables.

You must not use the IT facilities in a way that interferes with others' valid use of them.

1.9 Monitoring

The University of Brighton monitors and records the use of its IT facilities for the purposes of:

- The effective and efficient planning and operation of the IT facilities;
- Detection and prevention of infringement of these regulations;
- Investigation of alleged misconduct;
- The continuance of the legitimate business of the University in the absence of an employee

The University of Brighton will comply with lawful requests for information from government and law enforcement agencies.

You must not attempt to monitor the use of the IT facilities without explicit authority from the Director of Information Services.

1.10 Infringement

Infringing these regulations may result in sanctions under the institution's disciplinary processes for staff or students as appropriate. Penalties may include withdrawal of services and/or disciplinary action. Offending material will be removed.

Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.

The University of Brighton reserves the right to recover from you any costs incurred as a result of your infringement.

You must inform Information Services service desk (servicedesk@brighton.ac.uk) if you become aware of any infringement of these regulations.

2 Guidance notes

This guidance expands on the principles set out in the core regulations. It gives many examples of specific situations and is intended to help you relate your everyday use of the IT facilities to the *dos and don'ts* in the core regulations.

Where a list of examples is given, these are just some of the most common instances, and the list is not intended to be exhaustive.

Where the terms similar to Authority, Authorised, Approved or Approval appear, they refer to authority or approval originating from the person or body identified in *section 3, Authority* or anyone with authority delegated to them by that person or body.

2.1 Scope

2.1.1 Users

These regulations apply to **anyone** using the University of Brighton's IT facilities. This means more than students and staff. It could include, for example:

- Visitors to the University of Brighton web site, and people accessing the institution's online services from off campus;
- External partners, contractors and agents based on site and using the University of Brighton's network, or offsite and accessing the institution's systems;
- Tenants of the institution using the University's computers, servers or network;
- Visitors using the institution's Wi-Fi or other IT facilities;
- Students and staff from other organisations connecting using eduroam.

2.1.2 IT Facilities

The term IT Facilities include:

- IT Hardware that the University of Brighton provides, such as PCs, laptops, tablets, smart phones, and printers;
- Software that the institution provides, such as operating systems, office application software, web browsers etc. It also includes software that the institution has arranged for you to have access to, for example special deals for students on commercial application packages;
- Data that the University of Brighton provides, or arranges access to. This might include online journals, data sets or citation databases;

- Access to the network provided or arranged by the institution. This would cover, for example, network connections in halls of residence, on-campus Wi-Fi, connectivity to the internet from University PCs;

- Online services arranged by the institution such as Office 365, JSTOR, online library, or any of the Jisc online resources;

- *IT credentials*, such as the use of your institutional login, or any other token (email address, smartcard, PIN, dongle) issued by the University of Brighton to identify yourself when using IT facilities. For example, you may be able to use drop-in facilities or Wi-Fi connectivity at other institutions using your usual username and password through the eduroam system. While doing so, you are subject to these regulations, as well as the regulations at the institution you are visiting.

2.2 Governance

It is helpful to remember that using IT has consequences in the physical world.

Your use of IT is governed by IT-specific laws and regulations (such as these), but it is also subject to general laws and regulations such as your institution's general policies. These IT Regulations are governed by the IT Governance Board of the University of Brighton.

2.2.1 Domestic Law

Your behaviour is subject to the laws of the land, even those that are not directly related to IT such as the Prevent Duty, and laws on fraud, theft and harassment.

There are many items of legislation that are particularly relevant to the use of IT, including:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 2018
- General Data Protection Regulation (EU) 2016/679 (GDPR)

- Regulation of Investigatory Powers Act 2000
- Data Retention and Investigatory Powers Act 2014
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Counter-Terrorism and Security Act 2015
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002
- Equality Act 2010
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Defamation Act 1996 and 2013

So, for example, you may not:

- Create or transmit, or cause the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- Create or transmit material with the intent to cause annoyance, inconvenience or needless anxiety;
- Create or transmit material with the intent to defraud;
- Create or transmit defamatory material;
- Create or transmit material such that this infringes the copyright of another person or organisation;
- Create or transmit material that may cause people to be drawn into terrorism;
- Create or transmit unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their user organisation has chosen to subscribe;
- Deliberately (and without authorisation) access networked facilities or services.

2.2.2 Foreign Law

If you are using services that are hosted in a different part of the world or are consuming University services overseas, you may also be subject to their laws. It can be difficult to know where any particular service is hosted from, and what the applicable laws are in that locality. In general, if you apply common sense, obey domestic laws and the regulations of the service you are using, you are unlikely to go astray.

2.2.3 General Institutional Regulations

You should already be familiar with the University of Brighton's general regulations and policies. In particular you should be aware of and abide by the following policies as a minimum:

- University of Brighton Social Media Policy
- University of Brighton Data Protection policy
- Equality and Diversity Policy
- Human Resources policies, guidelines and procedures
- Information Services policies and procedures
- Student Services policies and procedures
- Prevent duty, legislation and guidance

All university polices are available at
https://staff.brighton.ac.uk/suppyou/Pages/policies.aspx

2.2.4 Third Party Regulations

If you use the University of Brighton's IT facilities to access third party services or resources you are bound by the regulations associated with that service or resource. (The association can be through something as simple as using your institutional username and password).

Very often, these regulations will be presented to you the first time you use the service, but in some cases the service is so pervasive that you will not even know that you are using it.

Two examples of this would be:

- **Using Janet, the IT network that connects all UK higher education and research institutions together and to the Internet** When connecting to any site outside the university of Brighton you will be using Janet, and subject to the Janet Acceptable Use Policy, https://community.ja.net/library/acceptable-use-policy the Janet Security Policy, https://community.ja.net/library/janet-policies/security-policy and the Janet Eligibility Policy https://community.ja.net/library/janet-policies/eligibility-policy. The requirements of these policies have been incorporated into these regulations, so if you abide by these regulations you should not infringe the Janet policies.

- **Using Chest agreements** Eduserv is an organisation that has negotiated many deals for software and online resources on behalf of the

UK higher education community, under the common banner of *Chest agreements*. These agreements have certain restrictions, that may be summarised as: non-academic use is not permitted; copyright must be respected; privileges granted under *Chest agreements* must not be passed on to third parties; and users must accept the User Acknowledgement of Third Party Rights, available at www.eduserv.org.uk/services/Chest-Agreements/about-our-licences/user-obligations

There will be other instances where the University of Brighton has provided you with a piece of software or a resource. Users shall only use software and other resources in compliance with all applicable contracts, licences, terms and conditions. You are responsible for ensuring that you do not breach these conditions.

2.3 Authority

These regulations are issued under the authority of the Director of Information Services who is also responsible for their interpretation and enforcement, and who may also delegate such authority to other people.

Authority to use the institution's IT facilities is granted by a variety of means:

- The issue of a username and password or other *IT credentials*
- The explicit granting of access rights to a specific system or resource
- The provision of a facility in an obviously *open access* setting, such as an Institutional web site; a self-service kiosk in a public area; or an open WiFi network on the campus.

If you have any doubt whether or not you have the authority to use an IT facility you should seek further advice from the IS service desk (servicedesk@brighton.ac.uk).

Attempting to use the IT facilities without the permission of the relevant authority is an offence under the Computer Misuse Act.

2.4 Intended Use

The University of Brighton's IT facilities, and the Janet network that connects institutions together and to the Internet, are funded by the tax-paying public. They have a right to know that the facilities are being used for the purposes for which they are intended.

2.4.1 Use for Purposes in Furtherance of Institution's Mission

The IT facilities are provided for use in furtherance of the institution's mission. Such use might be for learning, teaching, research, knowledge transfer, public outreach, the commercial activities of the institution, or the administration necessary to support all of the above.

2.4.2 Personal Use

You may currently use the IT facilities for personal use provided that it does not breach the regulations, and that it does not prevent or interfere with other people using the facilities for valid purposes (for example using a PC to update your Facebook page when others are waiting to complete their assignments). This is a concession and can be withdrawn at any time and staff using the IT facilities for non-work purposes during working hours are subject to the same management policies as for any other type of non-work activity. When using the facilities for personal activities be aware that in some circumstances your data may be provided to third parties as part of a legal obligation or as a result of other activity beyond the control of the University.

2.4.3 Commercial Use and Personal Gain

Use of IT facilities for non-institutional commercial purposes or for personal gain, such as running a club or society, requires the explicit approval of the Director of Information Services. The provider of the service may require a fee or a share of the income for this type of use. For more information, contact the IS Service Desk (servicedesk@brighton.ac.uk).

Even with such approval, the use of licences under the Chest agreements for anything other than teaching, studying or research, administration or management purposes is prohibited, and you must ensure that licences allowing commercial use are in place.

2.5 Identity

Many of the IT services provided or arranged by the institution require you to identify yourself so that the service *knows* that you are entitled to use it.

This is most commonly done by providing you with a username and password, but other forms of *IT credentials* may be used, such as an email address, a smart card or some other form of security device.

2.5.1 Passwords

2.5.1.1 Password Controls

Password controls are the principal means of ensuring that only authorised persons can access information. Passwords are only effective if they are:

- Good quality (see below)
- Never shared
- Changed periodically

Wherever possible, technical controls and settings have been implemented to ensure that good quality, complex passwords are in use (e.g. your network logon). Where it has not been possible, employees are still expected to follow the password policy stated here.

2.5.1.2 Rules for Password Selection

One of the following two options should be met in selecting a password for any University system:

1. Short but complex

- Minimum length 8 characters
- May not contain any word in the English Dictionary
- Must contain characters from three of the following four categories:
  1. English uppercase characters (A through Z)
  2. English lowercase characters (a through z)
  3. Base 10 digits (0 through 9)
  4. Non-alphabetic characters (for example, !, $, #, %)

2. Long

- Minimum length 16 characters
- made up of three or more non-related dictionary words
- e.g. 'christmasfinancialtaxi'

Tip: Both Long and Complex

- By using a sentence structure, with grammar in the phrase, it is possible to create a memorable password that is long and complex
- e.g. 'Oh when the saints go marching in!'
- Number substitutions can increase the complexity again e.g. 'Oh when the s4ints go m4rching in!'

Whichever option is chosen all passwords must:

- not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- be memorable, so you don't need to write it down
- unique to university systems. Do not use your password with any other account, especially social media, personal email, or retail websites.

2.5.1.3 Password Guidance

Passwords should follow the best practice guidance issued by the National Cyber Security Centre and are available at https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Consideration should also be given to the advice from the Information Commissioners office regarding passwords, particularly if you are developing software or operating a website, at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/

In addition, if you are using a password manager such as 1Password or Apple Keychain, you should ensure that access to these tools is managed using a multi-factor authentication capability and not just a simple password.

2.5.1.4 Keeping passwords safe

You must take all reasonable precautions to safeguard any *IT credentials* issued to you.

In order that passwords remain secure, the following advice is expected to be followed:

- Users are forbidden from sharing their passwords with anyone else
- Passwords must never be written down
- Passwords must never be stored in an unprotected file

If you think someone else has found out what your password is, change it immediately and report the matter to the IS Service Desk (servicedesk@brighton.ac.uk).

Do not use your username and password to log in to web sites or services you do not recognise, and do not log in to web sites that are not showing the padlock symbol.

Do not leave logged in computers unattended, and log out properly when you are finished.

Don't allow anyone else to use your smartcard or other security hardware. Take care not to lose them, and if you do, report the matter to the IS Service Desk (servicedesk@brighton.ac.uk) immediately.

It is recognised that it is sometimes difficult to remember passwords, particularly if they are long and complex. Whilst password management software tools can help, the University does not recommend any particular one. Should you choose to use one you are responsible for the safety and security of any IT credentials that you store within it.

There are a number of known exceptions to this policy. These are very much the exception and have been individually authorised. If any shared accounts are noticed, the Information Security Management Representative within your department or the IS Service Desk should be informed.

2.5.2 Impersonation

Never use someone else's *IT credentials*, or attempt to disguise or hide your real identity when using the institution's IT facilities. However, it is acceptable not to reveal your identity if the system or service clearly allows anonymous use (such as a public facing website).

2.5.3 Attempt to Compromise Others' Identities

You must not attempt to usurp, borrow, corrupt or destroy someone else's *IT credentials*.

2.6 Infrastructure and IT Assets

The IT infrastructure is all the underlying *elements* that makes IT function. It includes servers, the network, PCs, printers, operating systems, databases and a whole host of other hardware and software that has to be set up correctly to ensure the reliable, efficient and secure delivery of IT services.

You must not do anything to jeopardise the infrastructure.

2.6.1 Physical Damage or Risk of Damage

Do not damage, or do anything to risk physically damaging the infrastructure, such as being careless with food or drink at a PC, or playing football in a drop-in facility.

2.6.2 Reconfiguration

Do not attempt to change the setup of the infrastructure without authorisation, such as changing the network point that a PC is plugged in to, connecting devices to the network (except of course for Wi-Fi or Ethernet networks specifically designated for this purpose) or altering the configuration of the institution's PCs. Unless you have been authorised, you must not add software to or remove software from PCs.

Do not move equipment without authority.

2.6.3 Network Extension

You must not extend the wired or Wi-Fi network without authorisation. Such activities, which may involve the use of routers, repeaters, hubs or Wi-Fi access points, can disrupt the network and are likely to be in breach of the Janet Security Policy.

2.6.4 Setting up Servers

You must not set up any hardware or software that would provide a service to others over the network without permission. Examples would include games servers, file sharing services, IRC servers or web sites.

2.6.5 Introducing Malware

You must take all reasonable steps to avoid introducing malware to the infrastructure.

The term malware covers many things such as viruses, worms and Trojans, but is basically any software used to disrupt computer operation or subvert security. It is usually spread by visiting websites of a dubious nature, downloading files from untrusted sources, opening email attachments from people you do not know or inserting media that have been created on compromised computers.

If you avoid these types of behaviour, keep your anti-virus software up to date and switched on, and run scans of your computer on a regular basis, you should not fall foul of this problem.

2.6.6 Subverting Security Measures

The University of Brighton has taken measures to safeguard the security of its IT infrastructure, including things such as anti-virus software, firewalls, spam filters

and so on.

You must not attempt to subvert or circumvent these measures in any way.

2.7 Information Classification and Handling

2.7.1 Personal, Sensitive and Confidential Information

During the course of their work or studies, staff and students (particularly research students) may handle information that comes under the Data Protection Act 2018, or is sensitive or confidential in some other way. The Guidelines for Data Storage and Classification of Information set out the detail of data classification and handling but in the rest of this section, these will be grouped together as protected information.

Information included in this classification includes any of the following

- Any information with personal identifiable information (PII) which must therefore be afforded protection under the Data Protection Act:
  - Student records
  - Medical records
  - Personnel records (HR)
- Any information which could cause financial loss to the University or to users:
  - Payment card details
- Commercially sensitive information or intellectual property of the University:
  - Exam papers and scripts
  - Research documentation
- Information which should be restricted to certain groups of users within the University or it's departments, for example:
  - Management information (Directors)
  - Finance, payroll information (Finance)
  - Network connection details (IT)
  - Access details (IT)
- Any information which, if obtained by any non-authorised person employed by the University or otherwise, could reasonably be considered a security risk.

Safeguarding the security of protected information is a highly complex issue, with organisational, technical and human aspects. The institution has policies on Data Protection and Information Management (https://staff.brighton.ac.uk/reg/legal/Pages/home.aspx), and if your role is likely to involve handling protected information, you must make yourself familiar with and abide by these policies. Additional guidance on the provisions of the Data Protection Act 2018 and how the University of Brighton ensures compliance with it is available at https://staff.brighton.ac.uk/reg/legal/Pages/home.aspx.

2.7.1.1 Transmission of Protected Information

When sending protected information electronically, you must use a method with appropriate security. Email is not inherently secure. Advice about how to send protected information electronically is available from the IS Service Desk (servicedesk@brighton.ac.uk).

2.7.1.2 Storage on Portable Computers, Removable Media and Mobile Devices

Protected information must not be stored on removable media (such as USB storage devices, removable hard drives, CDs, DVDs) or mobile devices (laptops, tablet or smart phones) unless it is encrypted, and the key kept securely. If protected information is sent using removable media, you must use a secure, tracked service so that you know it has arrived safely. Advice on the use of removable media and mobile devices for protected information is available from the IS Service Desk (servicedesk@brighton.ac.uk).

The Information Commissioners Office provides guidance on encryption methods and uses at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/

2.7.1.3 Remote Working

If you access protected information from off campus, you must make sure you are using an approved connection method that ensures that the information cannot be intercepted between the device you are using and the source of the secure service.

Do not connect any University owned devices to any wireless network or a wireless network which is unsecured, unless the operator of the network is known. Be careful that the name is correct and not a close imitation e.g. 'Eduroam' rather than '_!Eduroam'.

If using a secure public network (e.g. a hotel wireless network), users should assume that all information transmitted could be seen by a third party. Encryption is needed to transfer any confidential information.

You must also be careful to avoid working in public locations where your screen can be seen. Laptops and mobile phones should be stored out of sight when not in use.

Take care when discussing confidential/sensitive matters in public places. Discussing confidential information should be avoided where possible in public places.

Advice on working remotely with protected information is available from the IS Service Desk (servicedesk@brighton.ac.uk)

2.7.1.4 Protected Information in Paper Form

Where protected or confidential information is in printed form, the following controls need to be adopted:

- When not in use, ***protected*** information should either be locked away, or must be stored in a room which is accessible only to those persons who have permission to access it.

- ***Protected*** information should not be left on desks overnight (a clear desk policy).

- Sending protected information by post should be avoided whenever possible. A reputable courier with package tracking must be used.

- Sending protected information by fax should be avoided whenever possible. When it is necessary, the recipient should be contacted to be made aware that the fax is being sent.

- When printing, paper should be picked up as soon as it is printed.

- Paper with protected information must be shredded when no longer required.

2.7.1.5 Personal or Public Devices and Cloud Services

Even if you are using approved connection methods, devices that are not fully managed by the University of Brighton cannot be guaranteed to be free of malicious software that could, for example, gather keyboard input and screen displays. You should not therefore use such devices to access, transmit or store protected information that might be subject to data protection legislation or be deemed confidential.

Advice on the use of personal devices to access institutional services is available from the Service Desk (servicedesk@brighton.ac.uk).

Cloud based tools supported by the University such as Office 365 have been assessed of the security and privacy implications, and you must comply with University guidance for their use.

Do not store protected information, such as personal or confidential information, in personal cloud services such as Dropbox unless securely encrypted first.

2.7.1.6 Unattended Equipment

Users are responsible for ensuring that unattended computer equipment is properly secured. Equipment, such as desktop computers or network file servers, are particularly vulnerable if left unattended for extended periods in a normal office environment. All employees and contractors should be made aware of the requirements and procedures for protecting unattended equipment, together with their responsibilities in this area.

It is expected that users lock their screens whenever they leave computer equipment unattended.

2.7.2 Copyright Information

Almost all published works are protected by copyright. If you are going to use material (images, text, music, software), the onus is on you to ensure that you use it within copyright law. This is a complex area, and training and guidance are available at https://staff.brighton.ac.uk/is/learningandteaching/Pages/Copyright/Copyright.aspx

The key point to remember is that the fact that you can see something on the web,

download it or otherwise access it does not mean that you can do what you want with it.

2.7.3 Others' Information

You must not attempt to access, delete, modify or disclose restricted information belonging to other people without their permission, unless it is obvious that they intend others to do this, or you have approval from the University's Legal Officer.

Private information may only be accessed by someone other than the owner under very specific circumstances governed by institutional and/or legal processes. Such requests must be referred to the University's Legal Officer or the Data Protection Officer for initial consideration.

Where information has been produced in the course of employment by the University of Brighton, and the person who created or manages it is unavailable, the responsible Director or Head of the organisational unit in which the person belongs may request permission for it to be retrieved for work purposes by following the Guidelines for accessing business communications when staff are absent. In doing so, care must be taken not to retrieve any private information in the account, nor to compromise the security of the account concerned.

It is not permissible to arrange automatic forwarding of email from an individual's mailbox to any other mailbox on behalf of another person. Individual mailbox forwarding is a decision that only the account nominee can make and setup and consideration should be given to what might be auto-forwarded as a result, such as emails from HR regarding absence, emails from Occupational Health regarding health conditions and other personal email. This applies regardless of whether the account nominee is still a member of the university or not.

2.7.4 Inappropriate Material & Research

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening or discriminatory.

The University of Brighton has procedures to approve and manage valid activities for research purposes that involve access to and/or storage of sensitive research material. When conducting research that may bring you into conflict with the IT regulations you must adhere to the sensitive research policy. In particular you must register your research activity in advance. For more information, please refer to the Section on 'Registration of Sensitive Research' at https://staff.brighton.ac.uk/ease/ro/Pages/Research_Integrity_Ethics.aspx and also

There is also an exemption covering authorised IT staff involved in the preservation of evidence for the purposes of investigating breaches of the regulations or the law.

2.7.5 Publishing Information

Publishing means the act of making information available to the general public, this includes through web sites, social networks and news feeds. Whilst the University of Brighton generally encourages publication, there are some general guidelines you should adhere to:

2.7.5.1 Representing the Institution

You must not make statements that purport to represent the University of Brighton without the approval of the University's Communications Manager within the Marketing and Communications department.

2.7.6 Publishing for Others

You must not publish information on behalf of third parties using the institution's IT facilities without the approval of the Director of Information Services.

2.8 Behaviour

The way you behave when using IT should be no different to how you would behave under other circumstances. Abusive, inconsiderate or discriminatory behaviour is unacceptable.

2.8.1 Conduct online and on social media

The University of Brighton's policies concerning staff and students also apply to the use of social media. These include human resource policies, codes of conduct, acceptable use of IT and disciplinary procedures.

2.8.2 Spam

You must not send unsolicited bulk emails or chain emails other than in specific circumstances. Advice on this is available from https://staff.brighton.ac.uk/is/computing/Pages/Email/spam.aspx.

2.8.3 Denying Others Access

If you are using shared IT facilities for personal or social purposes, you should vacate them if they are needed by others with work to do. Similarly, do not occupy specialist facilities unnecessarily if someone else needs them. Any use that ordinarily might cause the detriment of the service to others must not be undertaken without prior authority from the Director of Information Services.

2.8.4 Disturbing Others

When using shared spaces, remember that others have a right work without undue disturbance. Keep noise down (turn 'phones to silent if you are in a silent study area), do not obstruct passageways and be sensitive to what others around you might find offensive.

2.8.5 Excessive Consumption of Bandwidth / Resources

Use resources wisely. Don't consume excessive bandwidth by uploading or downloading more material (particularly video) than is necessary. Do not waste paper by printing more than is needed, or by printing single sided when double sided would do. Don't waste electricity by leaving equipment needlessly switched on.

2.9 Monitoring

2.9.1 Institutional Monitoring

The University of Brighton monitors and logs the use of its IT facilities for the purposes of:

- Detecting, investigating or preventing misuse of the facilities or breaches of the University's regulations;
- Monitoring the effective function of the facilities;
- Investigation of alleged misconduct;
- Compliance with legal and audit regulations such as PCI-DSS and the Prevent Duty.
- Fulfilling data subject requests

The University of Brighton will comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security.

For more information, please refer to the University of Brighton Information Security Policy.

2.9.2 Unauthorised Monitoring

You must not attempt to monitor the use of the IT without the explicit permission of the Director of Information Services.

This would include:

- Monitoring of network traffic;
- Network and/or device discovery;
- WiFi traffic capture;
- Installation of key-logging or screen-grabbing software that may affect users other than yourself;
- attempting to access system logs or servers or network equipment.

Where IT is itself the subject of study or research, special arrangements will have been made, and you should contact your course leader / research supervisor for more information.

2.10 Infringement

2.10.1 Security Incidents & Weaknesses

A security incident is an event which has occurred which is in breach of any policy or procedure designed to protect information. A security weakness is something that may result in a breach of policy or procedure if no action is taken.

It is vital that both are reported to allow suitable action to be taken by management. Users are expected to raise any perceived breach as soon as they see it, both to protect themselves and the organisation.

It should not be seen as telling tails or pointing fingers. It is a matter of ensuring that things are made right. Remember, if a significant breach does occur then jobs may well be put at risk through loss of contract, significant fine or loss of reputation.

If in doubt, raise it.

2.10.1.1 Definition of Incidents and Weaknesses

An information security incident or weakness is not just the obvious theft of laptops or phones. The following examples provide potential security breaches that should be reported. The list is not exhaustive.

Breaches of Confidentiality

- A user finds they are able to access some information which they feel they shouldn't (e.g. payroll information)
- A client emails personal information as an unsecured email attachment
- A laptop, phone or access badge has been lost or stolen
- Confidential paper is found on an unattended desk or left on a printer in a public area
- On getting to your office in the morning a window if found open, or the alarm is unset.

Breaches of Integrity

- Incorrect records are noted in a database
- A file on the shared drive won't open
- Paper records cannot be found in an expected location

Breaches of Availability

- A system or application is unavailable
- An important piece of information (e.g. a contract) cannot be found

2.10.1.2 Reporting Procedure

If any breach is suspected, then report it at the earliest possible opportunity to either your Departmental Information Security Representative or the IS Service Desk (servicedesk@brighton.ac.uk). It is preferable that this is done in writing (e.g. an email) to ensure it is not forgotten about. Simply state what you have seen, providing as much detail as you can.

2.10.2 Disciplinary Process and Sanctions

Where a breach of these regulations is considered to have come about through unacceptable behaviour, it will be handled by the University of Brighton's disciplinary processes for staff or students as appropriate. This could have a bearing on your future studies or employment with the institution and beyond.

Sanctions may be imposed if the disciplinary process finds that you have indeed breached the regulations, for example, imposition of restrictions on your use of IT facilities; removal of services; withdrawal of offending material; fines and recovery of any costs incurred by the University of Brighton as a result of the breach.

2.10.2.1 Reporting to Other Authorities

If the institution believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency.

2.10.2.2 Reporting to Other Organisations

If the institution believes that a breach of a third party's regulations has taken place, it may report the matter to that organisation.

2.10.2.3 Report Infringements

If you become aware of an infringement of these regulations, you must report the matter to the relevant authorities.