Guidance Notes to be used in conjunction with the regulations governing the use of University computing facilities (the ‘Computing Regulations’)

Purpose and Context

This guidance expands on the principles set out in the Computing Regulations https://www.hud.ac.uk/media/policydocuments/Computing-Regulations.pdf. It gives many examples of specific situations and is intended to help you relate your everyday use of the University computing facilities.

1 Scope

The Computing Regulations apply to anyone using the University computing facilities. This means more than students and staff. It could include, for example:

- Visitors to the University’s web site, and people accessing the University’s online services from off campus;
- External partners, contractors and agents based on site and using the University’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 University’s WiFi;
- Students and staff from other institutions logging on using eduroam.

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.

Definitions used in the Computing Regulations and in these guidance notes

Appropriate authority refers to the Director of Computing and Library Services in respect of the general computing facilities and to the dean of school or director or head of service in respect of specific computing facilities.

Computing facilities includes:

- IT hardware that the University provides, such as PCs, laptops, tablets, smart phones and printers;
- Software that the University 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 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 on-campus, WiFi, or connectivity to the internet from University PCs;
● Online services arranged by the University such as Office 365 and Google Apps, JSTOR, or any of the Jisc online resources; and
● IT credentials.

*General computing facilities* refers to computing facilities provided or arranged by Computing and Library Services.

*IT* refers to ‘information technology’, the common term used to refer to anything related to computing technology, such as hardware, software, networking, the internet or corresponding services and support.

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

*Specific computing facilities* refers to computing facilities provided or arranged and networks managed by a school or service.

*University computing facilities* means the general computing facilities and the specific computing facilities.

### 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 The University of Huddersfield’s general policies and regulations.

#### 2.1 Domestic Law

Your behaviour is subject to the laws of the land, even those that are not apparently related to IT such as the 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
- Terrorism Act 2006
- 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
● Counter-Terrorism and Security Act 2015
● General Data Protection Regulation 2016
● Data Protection Act 2018.

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 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.

The University has a zero-tolerance approach to acts which could incite or promote terrorist activity. It is also under a duty to prevent extremism under the Counter-Terrorism and Security Act 2015.

2.2 Foreign Law

If you are using services that are hosted in a different part of the world, 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.

2.3 General Institutional Regulations

You should already be familiar with the University’s general regulations and policies. These are available at https://www.hud.ac.uk/policies/
2.4 **Third Party Regulations**

If you use the University computing 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.

Some 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 you will be using Janet, and subject to the Janet Acceptable Use Policy, [https://community.jisc.ac.uk/library/acceptable-use-policy](https://community.jisc.ac.uk/library/acceptable-use-policy) the Janet Security Policy, [https://community.jisc.ac.uk/library/janet-policies/security-policy](https://community.jisc.ac.uk/library/janet-policies/security-policy) and the Janet Eligibility Policy [https://community.jisc.ac.uk/library/janet-policies/eligibility-policy](https://community.jisc.ac.uk/library/janet-policies/eligibility-policy)

  The requirements of these policies have been incorporated into the Computing Regulations and these guidance notes, so if you abide by the Computing 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, which 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 Obligations, available at [https://www.chest.ac.uk/user-obligations/](https://www.chest.ac.uk/user-obligations/)

- **Licence agreements**

There will be other instances where the University has provided you with a piece of software or a resource.

Users shall only use software and other resources in compliance with all applicable licences, terms and conditions.

3 **Authority**

Authority relating to general computing facilities lies with the Director of Computing and Library Services. Authority relating to specific computing facilities lies with the appropriate dean, director or head of service. These people are responsible for their interpretation and enforcement, and they may also delegate such authority to other people.

Authority to use the University computing 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 a University web site; a self-service kiosk in a public area; or an open WiFi network on campus.

Following enrolment, students are authorised to use systems appropriate to their course of study. Automatic authorisation for students is extended to include some specific computing facilities; in other cases it is necessary to obtain authorisation from local system managers.

Employees are authorised to use systems appropriate to their work. The University reserves the right to deny or revoke authorisation to use its computing facilities.

Those who are not students or employees of the University may be authorised to use University computing facilities at the absolute and sole discretion of the appropriate authority. Those who arrange access on behalf of persons who are not students or employees must ensure that they are made aware of the Computing Regulations and these guidance notes and that the user can be individually identified.

If you have any doubt whether or not you have the authority to use a University computing facility you should seek further advice from IT Support in Computing and Library Services.

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

4 Intended Use

The University computing facilities, and the Janet network that connects institutions together and to the Internet, are funded in part 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.

4.1 Use for Purposes in Furtherance of the University’s Mission

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

4.2 Personal Use

You may currently use the University computing facilities for personal use provided that it does not breach the Computing Regulations, and that it does not prevent or interfere with other people using the computing facilities for valid purposes (for example using a PC to update your Facebook page when others are waiting to complete their assignments).

However, this is a concession and can be withdrawn at any time.

Employees using the University computing facilities for non-work purposes during working hours are subject to the same HR policies as for any other type of non-work activity and should refer to the Staff Handbook for further information.

4.3 Commercial Use and Personal Gain

Use of University computing facilities for non-institutional commercial purposes or for personal gain, such as running a club or society, requires the explicit approval of the appropriate authority. 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 Director of Computing and Library Services or other appropriate authority.

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. This restriction includes work undertaken on behalf of a placement employer by a student.

5 Identity

Many of the computing services provided or arranged by the University 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 (issued at the time of authorisation) and password, but other forms of IT credentials may be used, such as an email address, a smart card or some other type of security device.

5.1 Protect Identity

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

You must change passwords when first issued and at regular intervals as instructed. You should not use obvious passwords, and do not record them where there is any likelihood of someone else finding them. Do not use the same password as you do for personal (i.e. non-institutional) accounts. Do not share passwords with anyone else, even IT staff, no matter how convenient and harmless it may seem. Further guidance on the choosing, using and protecting passwords can be found in the University’s IT Security Procedure Manual.

If you think someone else has found out what your password is, change it immediately and report the matter to IT Support.

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, even for short periods. You should always log out before leaving a computer unattended. Don’t forget to log out properly when you are finished.

Don’t allow anyone else to use your Campus card or other security hardware. Take care not to lose them, and if you do, report the matter to IT immediately.

5.2 Impersonation

Never use someone else’s IT credentials, or attempt to disguise or hide your real identity when using the University computing 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).

5.3 Attempt to Compromise Others’ Identities

You must not attempt to use, borrow, corrupt or destroy someone else’s IT credentials.

6. Infrastructure
The IT infrastructure is all the underlying items 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 IT infrastructure.

6.1 Physical Damage or Risk of Damage

Do not damage, or do anything to risk physically damaging the IT infrastructure, such as being careless with food or drink at a PC.

6.2 Reconfiguration

Do not attempt to change the setup of the IT 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 WiFi or wired networks specifically provided for this purpose) or altering the configuration of the University's PCs. Unless you have been authorised, you must not add software to or remove software from PCs.

Do not move equipment without authority.

6.3 Network Extension

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

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.

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.

6.6 Subverting Security Measures

The University 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.

7 Information
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 relevant Data Protection Act and the General Data Protection Regulation, or is sensitive or confidential in some other way. For the rest of this section, these will be grouped together and described as ‘protected information’.

Safeguarding the security of protected information is a highly complex issue, with organisational, technical and human aspects. The University has policies and procedures on Data Protection and information governance generally, including in relation to Research Data Management and Records Management, 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 relevant Data Protection legislation and how The University of Huddersfield ensures compliance with it is available at: [http://www.hud.ac.uk/informationgovernance/dataprotection/](http://www.hud.ac.uk/informationgovernance/dataprotection/).

### 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 and should not be used to transfer University payment card details; instead use the phone or fax the details. Advice about how to send protected information electronically is available in The University of Huddersfield’s [IT Security Policy](http://www.hud.ac.uk/it/securitypolicy/) and in the [IT Security Procedure Manual](http://www.hud.ac.uk/it/proceduremanual/) and from IT Support [http://www.hud.ac.uk/it/contact/](http://www.hud.ac.uk/it/contact/).

### 7.1.2 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 or password-protected, and the key kept securely. A backup copy should also be kept.

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 in The University of Huddersfield’s [IT Security Policy](http://www.hud.ac.uk/it/securitypolicy/) and in the [IT Security Procedure Manual](http://www.hud.ac.uk/it/proceduremanual/) and from IT Support [http://www.hud.ac.uk/it/contact/](http://www.hud.ac.uk/it/contact/).

### 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.

You must also be careful to avoid working in public locations where your screen can be seen.

Advice on working remotely with protected information is available in the University’s [IT Security Policy](http://www.hud.ac.uk/it/securitypolicy/) and in the [IT Security Procedure Manual](http://www.hud.ac.uk/it/proceduremanual/) and from IT Support [http://www.hud.ac.uk/it/contact/](http://www.hud.ac.uk/it/contact/).

### 7.1.4 Personal or Public Devices and Cloud Services
Even if you are using approved connection methods, devices that are not fully managed by the University 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.

For further details, please consult the Using Your Own Device policy.

Do not store protected information in personal cloud services such as Dropbox. Cloud computing using generic services such as Dropbox is not currently compliant with data protection legislation, particularly given that data stored by such providers is likely to be transferred outside of the European Economic Area. It is therefore not appropriate for the storage of personal data relating to staff, students or research subjects. If you require any further guidance on using cloud computing services for the storage of information, you should contact IT Support.

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 guidance is available at https://library2.hud.ac.uk/pages/copyright/. 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.

7.3 Others’ Information

You must not attempt to access, delete, modify or disclose protected information belonging to other people (including data, emails, software, systems or services) without their permission, unless it is obvious that they intend others to do this, or you are specifically authorised to do so in writing by the appropriate authority. All users must restrict the use of such data to the purpose defined. Accessing personal data stored on a computer as a precursor to committing a criminal act is a criminal act in itself.

Where information has been produced in the course of employment by the University and the person who created or manages it is unavailable, the responsible line manager may give permission for it to be retrieved for work purposes. 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.

Private information may only be accessed by someone other than the owner under very specific circumstances governed by institutional and/or legal processes. Further information about the monitoring of e-mail and internet use by staff can be found in the Staff Handbook.

7.4 Inappropriate Material

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

The University of Huddersfield has procedures to approve and manage valid activities involving such material for valid research purposes where legal and with the appropriate ethical approval. For more information, please refer to the relevant School ethics committee.

There is also an exemption covering authorised IT staff involved in the preservation of evidence for the purposes of investigating breaches of the University’s policies and
procedures relating to the computing facilities, including the Computing Regulations, or breaches of the law.

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 generally encourages publication, there are some general guidelines you should adhere to:

7.5.1 **Representing the University**

You must not make statements that purport to represent the University without the approval of the appropriate University authority.

The University logo must not be used for staff or student personal work or communications. It can, however, be used for student final-year work, project work or research posters.

You must abide by the law and by these regulations when engaged in sending internal or external e-mail. Having a University email address is a privilege akin to using a University letterhead and you must not debase the reputation of the University. You must be certain that e-mail has an entirely legitimate purpose and that it will not cause offence or nuisance.

7.5.2 **Publishing for Others**

You must not publish information on behalf of third parties using the University computing facilities without the approval of the appropriate authority.

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.

8.1 **Conduct online and on social media**

The University’s policies concerning staff and students also apply to the use of social media and you must familiarise yourself with the University’s Social Media Policies. Other relevant policies include human resource policies, codes of conduct, acceptable use of IT and disciplinary procedures.

8.2 **Spam**

You must not send unsolicited bulk emails or chain emails other than in specific circumstances. Advice on this is available from IT Support.

8.3 **Denying Others Access**

If you are using shared computing facilities for personal or social purposes, you should vacate them if they are needed by others with work to do. Similarly, do not occupy
8.4 Disturbing Others

When using shared spaces, remember that others have a right to 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.

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.

9 Monitoring and Privacy

9.1 Institutional Monitoring

The University respects the privacy of its users and abides by the Regulation of Investigatory Powers Act 2000.

At the University, there is no routine monitoring of e-mail content or individual web use, although all web activity is logged, and access to sites which are likely to cause a breach of these regulations may be blocked. However, the Director of Computing and Library Services or other appropriate authority reserves the right to sanction investigation and inspection of electronic communications, under the terms of the Act, particularly where there is suspicion, or there appears to be evidence, of an infringement of the regulations or of illegal activity.

In addition to the above, the University monitors and logs the use of the University computing facilities for the purposes of monitoring the effective function of the facilities and their use by staff, students and others.

The University 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.

Except as may be required by law, the University accepts no liability for any consequences whether direct, indirect or consequential, arising from a breach of privacy, no matter how caused and whether or not such breach was within the control of the University.

9.2 Unauthorised Monitoring

You must not attempt to monitor the use of the University computing facilities without the explicit permission of the appropriate authority.

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.

10 Infringement

10.1 Disciplinary Process and Sanctions

Breaches of the Computing Regulations will be handled by the University’s disciplinary procedures. For students, further details are available in Section 7 of the Students’ Handbook of Regulations [http://www.hud.ac.uk/registry/regulationsandpolicies/studentregs/] for staff further details are available at [http://hr.hud.ac.uk/downloads/policies/pdf/1000094.pdf].

This could have a bearing on your future studies or employment with the University 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 University computing facilities; removal of services; withdrawal of offending material; fines and recovery of any costs incurred by the University as a result of the breach. Details of the sanctions that may be applied by the University under its Student Disciplinary Procedure are set out in the Students’ Handbook of Regulations [http://www.hud.ac.uk/registry/regulationsandpolicies/studentregs/]

10.2 Reporting to Other Authorities

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

10.3 Reporting to Other Organisations

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

10.4 Report Infringements

If you become aware of an infringement of these regulations, you must report the matter to a member of staff in Computing and Library Services or the appropriate authority.
## POLICY SIGN-OFF AND OWNERSHIP DETAILS

<table>
<thead>
<tr>
<th>Document name:</th>
<th>it regs (guidance) - 2019.docx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version Number:</td>
<td>1.2</td>
</tr>
<tr>
<td>Equality Impact Assessment:</td>
<td>March 2017</td>
</tr>
<tr>
<td>Approved by:</td>
<td>UTLC 22/05/2019</td>
</tr>
<tr>
<td>Effective from:</td>
<td>22/05/2019</td>
</tr>
<tr>
<td>Date for Review:</td>
<td>Mays 2020</td>
</tr>
<tr>
<td>Author:</td>
<td>Derek Heathcote</td>
</tr>
<tr>
<td>Owner (if different from above):</td>
<td>Krish Pilicudale, Head of IT and Deputy Director Computing and Library Services</td>
</tr>
<tr>
<td>Document Location:</td>
<td></td>
</tr>
<tr>
<td>Compliance Checks:</td>
<td>Breaches of the Regulations handled under the respective student or staff University disciplinary processes.</td>
</tr>
<tr>
<td>Related Policies/Procedures:</td>
<td>IT Security Policy</td>
</tr>
<tr>
<td></td>
<td>Using Your Own Device Policy</td>
</tr>
</tbody>
</table>

## REVISION HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Revision description/Summary of changes</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>April 2017</td>
<td>First draft using the Policy Framework. Minor updates, including reference to the Using Your Own Device policy.</td>
<td>Derek Heathcote</td>
</tr>
<tr>
<td>V1.1</td>
<td>February/March 2018</td>
<td>Inclusion of GDPR. Minor updates.</td>
<td>Derek Heathcote</td>
</tr>
<tr>
<td>V1.2</td>
<td>February/March 2019</td>
<td>Annual review. Minor updates only.</td>
<td>Derek Heathcote</td>
</tr>
</tbody>
</table>