Acceptable Use Policy

Document Control

Version	Author	Summary of Changes	Approved By	Date Published	Date of Review
1	MPI	New policy	F&O Committee	Feb 2023	Feb 2025

Contents

1.0 Purpose and Scope

1.1 These Conditions of Computer Use are a formal statement of what is acceptable and unacceptable when using the Trust's IT facilities and network. They aim to encourage responsible behaviour and good practice, thus assisting the Trust in maintaining a secure, safe and robust IT environment. The conditions detailed here apply to all using the Trust's IT facilities whether it be a member of staff, a student, governor, volunteers, contractors or a person from outside the Trust who has been authorised to use facilities.

1.2 All those using the Trust's IT facilities and network should be aware of these conditions and abide by them. Contravention of these conditions could lead to loss of access to IT facilities and disciplinary action. If you are unsure about any aspect of these Conditions of Use or your use of Trust's IT facilities, it is your responsibility to seek clarification by contacting the IT Dept

2.0 Summary of Conditions

2.1 Your Trust IT password is confidential and you must never disclose it to others, or let anyone else access services and systems using your password. Disclosing your password to others contravenes the Conditions of Computer Use and could lead to disciplinary action and loss of access to IT facilities.

2.2 You should not respond to any request to disclose your password including those purporting to come from the IT dept.

2.3 Be aware of relevant legislation. In particular, if you work with personal information about individuals, you must be aware of and comply with the Data Protection Act and also the Prevent Duty.

2.4 Computing facilities are provided for Trust work purposes. Limited personal use is permitted, provided it is not illegal, does not adversely affect other users, does not interfere with work or studies, or in any other way breach the Conditions of Computer Use. Staff should not use the Trust email service for personal (non-work related) emails.

2.5 Care must be taken to ensure you do not create, transmit or publish any material that is extremist, illegal, offensive, abusive, or whose effect is to bring the Trust into disrepute.

2.6 Files are private. You must not attempt to access files or computer systems which you are not authorised to access.

2.7 Electronic media are subject to copyright. It is illegal to make an electronic copy (e.g. by scanning, downloading, copying from disk etc.) unless you have the appropriate copyright authorisation.

2.8 Software is subject to copyright and licensing restrictions. Software provided by the Trust should only be used by members of the Trust for Trust purposes and in accordance with licence conditions of the software. You should not install, copy or distribute it to others unless authorised to do so.

2.9 Care must be taken when introducing software/data into the Trust. Only those authorised to do so should install data or software onto Trust-owned devices and they should ensure it has been checked for viruses or other malware.

2.10 Where necessary, administrative rights may be granted to permit users to install software on Trust devices. Do not transmit files/data to others without first checking for viruses or other malware.

2.11 If you are responsible for supporting others and the systems and services they use, you have an additional responsibility to ensure that those systems and services are secure, and should encourage good practice in those that use them.

2.12 All personally-owned electronic devices connected to the network are the owner's responsibility. They are responsible for security of that system and any activity on it. Should inappropriate activity be detected

arising from the device, the registered owner will be held responsible for that activity. The owner should ensure that the system has up to date operating system and application software security patches applied and where feasible up to date anti-virus/anti-malware software is installed. Refer to the Trust's Bring Your Own Device (BYOD) policy for further information and guidance.

2.13 Use of Trust computer systems and the network is monitored. The Trust has the right to access files, intercept communications, or monitor usage where there are grounds for suspecting mis-use which if proven could result in disciplinary action being taken. In cases where illegal activity is involved copies of relevant information may be handed to the Police at their request.

3.0 Conditions of Use

3.1 Full use of the Trust's IT facilities and network is restricted to the following registered users authenticating by means of a Trust IT account:

- Students registered with the Trust for a programme of study.
- Staff holding a contract of employment with the Trust.
- Other individuals e.g. Volunteers who have registered with Trust

All of the above must have signed up to and agreed to the Trust Acceptable Computer Use Agreement

3.2 All users of the Trust's IT facilities are bound by current relevant legislation.

Computer Misuse Act 1990

Communications Act 2003

Regulation of Investigatory Powers Act 2000

Anti-terrorism, Crime and Security Act 2001

Counter Terrorism Act 2015

Prevent Duty 2015

Freedom of Information Act 2000

The Education and Inspections Act 2006

Keeping Children Safe in Education 2018

General Data Protection Regulation (GDPR)

3.3 Computing facilities are provided for the pursuit of legitimate Trust activities:

- Teaching and learning.
- Personal educational development.
- Administration and management of Trust business.
- Limited use of the Trust network and IT facilities for personal purposes other than Trust work or study, for instance access to the internet, is permitted. However, such use must not interfere with work or studies, must be legal and must be strictly in accordance with the requirements laid down in these Conditions of Computer Use.

4.0 Unacceptable use

4.1 All of the following are expressly forbidden when using the Trust's network and IT facilities:

- Any illegal purposes. The Police will be informed where there is evidence of illegal activity
- Accessing, creating, storing or transmitting offensive, obscene or indecent data or images or data from which such material could be derived, or material that might be subject to the provisions of counter-terrorism legislation
- Creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- Creation, transmission or distribution of materials in relation to radical or extremist views
- Creation or transmission of defamatory, discriminatory or libellous material, or material whose effect is to bring the Trust into disrepute
- Transmission of material that infringes the copyright of another person
- The unauthorised distribution to third parties of any information in which the Trust and/or partner organisations have intellectual property rights
- Unauthorised interception or hacking of communications over the network including but not limited to e-mail and telephone messages
- The transmission of unsolicited commercial or advertising material either within the Trust or externally, unless authorised to do so on behalf of the Trust
- Unauthorised access or attempting to gain unauthorised access to IT facilities or services both within and outside the Trust
- Disclosing your Trust password to others, or letting others use your Trust IT account
- Research using radical or extremist sites for the purpose of the curriculum being delivered needs clear evidence to support why such sites need to be accessed.

4.2 Users are responsible for the security of their password and should under no circumstances disclose this to others, whether in response to an e-mail, by visiting a web page, in person, or over the telephone; neither should they allow others to use their IT account.

4.3 Deliberate activities with any of the following characteristics are prohibited:

- Corrupting or destroying others users' data
- Violating the privacy of others.
- Disrupting the work of others.
- Bullying or harassing others.
- Causing annoyance to others by inappropriate or inconsiderate use of computing facilities (e.g. internet phones in IT areas).
- Using applications for non-academic purposes which are likely to result in excessive network traffic causing disruption to others.
- Continuing to use an item of software/hardware after IT Services has requested that such use cease.
- Misuse of Trust IT facilities or resources in such a manner that it compromises the security of Trust systems and the network.

5.0 Software

5.1 Software is subject to copyright and licensing restrictions and persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.

5.2 Software provided by the Trust should only be used in accordance with license conditions of the software. You should not copy or distribute it to others unless authorised to do so.

5.3 Software provided by the Trust should not be deleted, disabled or altered, other than by authorised personnel.

5.4 Leaving members of staff or students must remove any copies of Trust software installed on their personnel devices prior to leaving the Trust.

6.0 Computer security

6.1 All access to computers and the network should be authenticated by means of a Username and Password.

6.2 Computer log on passwords must be at least 14 characters long and must be changed at least every 12 months to maintain security.

6.3 All IT equipment in the Trust should be maintained in a secure manner.

6.4 All devices connected to the Trust's campus wired network should run a currently supported operating system. All devices should have up to date operating system and application software security patches applied and where feasible anti-virus/anti-malware software installed, irrespective of whether they are owned by the Trust, or personally owned.

6.5 Only those authorised to do so should install data or software onto Trust owned devices and they should ensure it has been checked for viruses or other malware.

6.6 Users should not transmit files/data to others, without first checking for viruses or other malware.

6.7 Information Services reserves the right to disconnect any computer from the network that is discovered to be infected with malware (e.g. viruses, trojans), or does not have adequate virus-checking software installed. The associated password should be reset on an uninfected machine. Once cleaned, the device can be reconnected to the network.

7.0 Connecting equipment to the network

7.1 No equipment (whether Trust or user owned) should be used to extend or provide additional connections, for example via wireless transmitters or routers, unless approved for this purpose by IT Services.

7.2 The Trust reserves the right to prohibit the use of equipment which is likely to cause interference on frequency ranges used by the Trust's wireless network.

7.3 The registered owner of a device will be held responsible for any inappropriate activity arising from that device

7.4 In the case of personally-owned systems the owner is responsible for ensuring that the device has up to date operating system and application software security patches applied, and where feasible up to date anti-virus/anti-malware software is installed.

8.0 Electronic mail

8.1 Staff should not use Trust's e-mail systems for sending personal messages unrelated to Trust matters.

8.2 E-mail systems provide a written record and care should be taken when composing and sending messages to ensure that the intended meaning is conveyed and the message is delivered to the intended recipients.

8.3 The Data Protection and Freedom of Information Acts also apply to e-mails. Such e-mails must be stored and processed in accordance with the Data Protection Act and may have to be released in response to Freedom of Information Act requests.

8.4 E-mails which infringe the copyright of another person should not be passed on.

8.5 Anything sent electronically, including e-mail, is susceptible to interception. Users should whenever possible avoid sending highly confidential or sensitive information by e-mail. If it is essential to do so, the information should be contained within a password protected file attached to the message. The password should be communicated to the intended recipient by other means.

8.6 Users should never send their Trust password in an e-mail. Any e-mail which asks for your password is a hoax.

8.7 Before sending an e-mail users should assess whether the message is representing Trust views and whether the information is confidential, and make this clear within the message.

8.8 Users should note that their use of the Trust e-mail system is not private and that whilst continuing to maintain the privacy of personal mail, the Trust reserves the right to inspect and disclose the contents of e-mails under special circumstances.

8.9 Files downloaded from the internet, including mobile code and files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.

9.0 Personal Use

9.1 Staff are permitted to occasionally use Trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Trust may withdraw permission for it at any time or restrict access at their discretion.

9.2 Personal use is permitted provided that such use:

- Does not take place during contact time, teaching hours, non-break time.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

9.3 Staff may not use the Trust's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

9.4 Staff should be aware that use of the Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities (see section 12). Where breaches of this policy are found, disciplinary action may be taken.

9.5 Staff should be aware that personal use of ICT (even when not using Trust's ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them. Staff should take care to follow the Trust's policy and guidelines on social media and use of email (see section 8) to protect themselves online and avoid compromising their professional integrity.

10.0 Internet publishing

10.1 Users should be aware that sending electronic mail to any extended group including but not limited to social networking sites and blogs, or even to a list of recipients, is considered to constitute its publication. Likewise, placing information onto a computing system in such a way as to make it accessible via the World Wide Web is considered to constitute its publication.

10.2 No item should be published using the Trust's facilities that could be considered to be defamatory, discreditable or injurious to the Trust's reputation, that in any way contravenes current legislation. The Trust

reserves the right to remove any such material and to remove access rights in order to prevent further publishing of such material.

11.0 Visitors

11.1 Visitors must not intentionally contravene these Trust Conditions of Computer Use in any way.

11.2 Visitors should not attempt to run any software whose use is prohibited by the Trust, either on their own system connected to the Trust network, or on Trust-owned systems.

11.3 Visitors must not disclose to anyone else passwords which have been allocated to them for the purpose of authorised access to Trust IT and computer systems.

11.4 Visitors must not take any action to circumvent any Trust security control that is in place.

12.0 Monitoring and Privacy

12.1 The Trust reserves the right to monitor use of the Trust's IT network, associated telecommunication systems and the Internet by users and, if necessary, to withdraw access if it is felt that it is being used excessively for purposes unconnected with and/or to the detriment of work/studies.

12.2 Routine monitoring takes place for maintenance, fault-finding purposes and enforcement of these Conditions of Computer Use, which may reveal unencrypted data and sites visited by users to operational staff. More detailed monitoring may also be undertaken if there are reasonable grounds to believe that a user has committed a criminal offence or is otherwise in breach of the Conditions of Computer Use.

12.3 Users should note that Trust facilities are provided primarily for Trust work, study and business purposes and that whilst continuing to maintain the privacy of personal information, the Trust reserves the right to process information stored on Trust IT systems, including the content of e-mails, web pages and files under the following circumstances:

- To locate substantive information that is required for Trust business.
- To set up an automatic reply or forward mail if members of staff are unexpectedly absent or have gone on leave without making forwarding arrangements.
- In the course of an investigation triggered by indications or allegations of misconduct, misuse, or illegal use.
- To respond to legal processes, or to fulfil the Trust's obligations to third parties or in other exceptional circumstances, e.g. medical emergency

12.4 The Trust's internet connection is secured. The Trust uses a firewall to filter, monitor and log all internet traffic from all devices connected to the Trust ICT network. This includes the Guest Wi-Fi network which personal devices may be connect to.

13.0 Breaches of these Conditions of Use

13.1 If there are reasonable grounds for suspecting that a user is engaging in activities which are in breach of the Conditions of Computer Use, the Trust reserves the right to investigate fully, including directly monitoring use of the network and computing facilities by the user. The Trust also reserves the right to withdraw (either temporarily or permanently) the authority of any user to use any system in such circumstances. Direct monitoring of individual use and/or withdrawal of services in such circumstances may be authorised only by the CEO, or their authorised deputies.

13.2 A breach of these conditions of use may lead to disciplinary proceedings and, in serious cases, dismissal for staff and exclusion for students. (A significant breach of these conditions of use is likely to be regarded as serious or gross misconduct.) A breach of these conditions of use may also constitute a criminal offence and the Trust will report the matter to the Police where appropriate.

14.0 Reporting Computer Misuse

14.1 Computer misuse is any activity involving the Trust's computing resources which is illegal, contravenes these Conditions of Computer Use, or has any of the following characteristics:

- Compromises the security of the Trust's IT systems or its data
- Results in a formal complaint from a member of the public or another member of the Trust
- Radical or extremist links
- Is part of a Police enquiry.

14.2 If a member of the Trust becomes aware of such activity, they have a responsibility to report this to IT Dept.

15.0 Advice and Clarification

Should you need any advice and/ or clarification of these Conditions of Computer Use then please contact the IT Dept in the first instance.

16.0 Signed Declaration

Please complete the section below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not agree to this agreement, access will not be granted to Trust ICT systems.

I have read and understand the above and agree to use the Trust ICT systems and when using my own device to access Trust ICT systems or data.

Name Printed ……

Signed ……

Date ……