Acceptable use of ICT policy

Approved by:	Chief Executive Officer	Date: September 2020
Last reviewed:	August 2020	
Next review due by:	July 2022	

The need for a policy

All Unity Schools Partnership's information communication technology (ICT) facilities and information resources remain the property of Unity Schools Partnership ("the Trust") and not of particular individuals, teams or departments. By following this policy we will help ensure that ICT facilities are used:

- legally;

- securely;

- safely

- without undermining the Trust or bringing it into disrepute;

- effectively;

- in a spirit of co-operation, trust and consideration for others;

- so that they remain available.

The policy relates to all ICT facilities and services provided by the Trust, although special emphasis is placed on email and the internet. All employees, volunteers, and any other users of our IT are expected to adhere to this policy.

1. **Disciplinary measures**

    1.1. Deliberate and serious breach of the policy statements in this section may lead to the Trust taking disciplinary measures in accordance with the disciplinary policy and procedure. The Trust accepts that ICT – especially cloud-based systems, for example but not limited to cloud storage, applications and email systems – are a valuable business tool. However, misuse of these facilities can have a negative impact upon employees' and volunteers' productivity and the reputation of the Trust.

    1.2. In addition, all the Trust's phone, web-based, locally hosted systems and email related resources are provided for business purposes. Therefore, the Trust maintains the right to monitor all internet and local network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use. However, see the Safeguarding section below.

2. **Safeguarding**

    2.1. Schools have a statutory duty to monitor their digital environment in order to identify any potential threats to pupils' welfare and wellbeing. The Trust's schools have appropriate filtering and monitoring in place.

    2.2. At Langer Primary Academy and in the Trust's secondary schools (including Churchill and Sir Bobby Robson) this monitoring is carried out by eSafe. eSafe combines intelligent detection software, expert human behaviour analysis and dynamic threat libraries to identify a range of safeguarding risks.

    2.3. In schools using eSafe all school owned devices will be continuously monitored for safeguarding risks. If pupils and staff use a school owned device outside of school, the device will continue to be monitored when it is both online and offline.

    2.4. A Data Protection Impact Assessment (DPIA) has been completed for eSafe and an addendum added to the staff, pupil and volunteer privacy notices.

2.5. Schools not using eSafe regularly (at least half-termly) review the logs produced by their filters. Monitoring what is trapped by the filter allows schools to identify individuals using inappropriate search terms, so that they can be given advice/support, and to see any trends, which can be used to inform the school's curriculum/advice to staff, pupils and parents/carers.

3. Security

3.1. As a user of the Trust's equipment and services, you are responsible for your activity.

3.2. <u>Do not disclose personal system passwords or other security details to other employees, volunteers or external agents, and do not use anyone else's log-in; this compromises the security of the Trust</u>. If someone else gets to know your password, ensure that you change it or get IT Services to help you.

3.3. If you intend to leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorised access. If you fail to do this, you will be responsible for any misuse of it while you are away. Logging off is especially important where members of the public have access to the screen in your absence.

3.4. Any pen drives or other storage devices used on the Trust's network should be secure. Please see paragraph 9 for more detail.

3.5. Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you do not have access to information or resources you feel you need, contact your line manager.

4. Use of Email

4.1. When to use email:

4.1.1. Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use.

4.1.2. Use the phone for urgent messages (email is a good backup in such instances). Use of email by employees and volunteers of the Trust is permitted and encouraged where such use supports the goals and objectives of the Trust.

4.1.3. However, the Trust has a policy for the use of email whereby employees and volunteers must ensure that they:

4.1.3.1. comply with current legislation;

4.1.3.2. use email in an acceptable way;

4.1.3.3. do not create unnecessary business risk to the Trust by their misuse of the internet.

4.2. Unacceptable behaviour

4.2.1. Sending confidential information to external locations without appropriate safeguards in place. See paragraph 6 of this document for more details.

4.2.2. Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.

4.2.3. Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying.

4.2.4. Using copyrighted information in a way that violates the copyright.

4.2.5. Breaking into the Trust's or another organisation's system, or unauthorised use of a password / mailbox.

4.2.6. Broadcasting unsolicited personal views on social, political, religious or other non-business-related matters.

4.2.7. Transmitting unsolicited commercial or advertising material.

4.2.8. Undertaking deliberate activities that waste employee's or volunteer's effort or networked resources.

4.2.9. Deliberately or recklessly introducing any form of computer virus or malware into the corporate network.

4.3. Confidentiality

Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. The Trust reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (employees, volunteers and temporary employees) within and outside the system as well as deleted messages. See paragraph 6 for more detail.

4.4. General points on email use

4.4.1. When publishing or transmitting information externally be aware that you are representing the Trust and could be seen as speaking on the Trust's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager;

4.4.2. Check your inbox at regular intervals during the working day. Keep your inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical);

4.4.3. Keep electronic files of electronic correspondence, only retaining what you need to. Do not print it off and keep paper files unless absolutely necessary;

4.4.4. Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague);

4.4.5. Do not forward emails warning about viruses (they are invariably hoaxes and IT Services will probably already be aware of genuine viruses – if in doubt, contact them for advice);

4.4.6. Do not open an email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. Alert IT Services if you are sent anything like this unexpectedly; this is one of

the most effective means of protecting the Trust against email virus and phishing attacks.

4.5. Email signatures

Keep these short and include your name, title, phone number(s) and website address.

5. Use of the Internet

5.1. Use of the Internet by employees and volunteers is permitted and encouraged where such use supports the goals and objectives of the school/Trust.

5.2. However, when using the Internet, employees and volunteers must ensure that they:

5.2.1. comply with current legislation;

5.2.2. use the internet in an acceptable way;

5.2.3. do not create unnecessary business risk to the Trust by their misuse of the internet.

5.3. Unacceptable behaviour

5.3.1. In particular the following is deemed unacceptable use or behaviour by employees and volunteers (this list is non-exhaustive):

5.3.1.1. Visiting internet sites that contain obscene, hateful, pornographic or other illegal material;

5.3.1.2. Using the computer to perpetrate any form of fraud, or software, film or music piracy;

5.3.1.3. Using the internet to send offensive or harassing material to other users;

5.3.1.4. Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;

5.3.1.5. Hacking into unauthorised areas;

5.3.1.6. Creating or transmitting defamatory material;

5.3.1.7. Undertaking deliberate activities that waste employee's or volunteer's effort or networked resources;

5.3.1.8. Deliberately or recklessly introducing any form of computer virus into the Trust's network.

5.4. Internet chat / instant messaging (IM) / video calling and conferencing

The use of internet chat, instant messaging and video calling and conferencing is permitted for business use only. This use must have been agreed with your line manager.

5.5. Webmail

The use of personal webmail (e.g. Hotmail, Google) is not permitted in the Trust unless previously agreed with your line manager and IT Services.

5.6. Obscenities / pornography

Do not write, publish, look for, bookmark, access or download material that might be

regarded as obscene or pornographic.

5.7. Copyright

    5.7.1. Take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

    5.7.2. Be aware of copyright law when using content you have found on other organisations' websites. The law is the same as it is for printed materials.

6. **Confidentiality**

6.1. If you are dealing with personal, sensitive and / or confidential information, then you must ensure that extra care is taken to protect the information. It must not be left unattended on printers, photocopiers or other reprographic facilities.

6.2. If sending personal, sensitive and / or confidential information via email, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, please check with IT Services.

    6.2.1. Personal, sensitive and / or confidential information should be contained in an attachment;

    6.2.2. In appropriate cases the attachment should be encrypted, and / or password protected;

    6.2.3. Any password or key must be sent separately; and preferably communicated by another means e.g. telephone, text message.

    6.2.4. Before sending the email, verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent;

    6.2.5. Do not refer to the information in the subject of the email.

7. **The Trust's network and cloud storage**

7.1. Keep master copies of important data on the Trust's network server or authorised Trust cloud storage, e.g. Microsoft One Drive or Google Drive and not solely on your PC's local C: Drive or portable disks. Not storing data on the Trust's network servers or cloud storage means it will not be backed up and is therefore at risk.

7.2. Ask for advice from IT Services if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can bring the network to a standstill.

7.3. Do not store personal (non-Unity Schools Partnership) files on the Trust's network or cloud storage.

7.4. Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

8. **Cloud File Sharing**

8.1. If sharing files held in cloud storage, e.g. Microsoft One Drive or Google Drive, ensure that the correct sharing permissions are set, e.g. view or edit and always select the most restrictive.

8.2. Ensure files are shared with the minimum number of recipients and consider if sharing is appropriate as your file could be further shared beyond your control.

8.3. Only share files internally. Permission to share files externally requires the approval of SLT (Senior Leadership Team).

8.4. Actively manage you sharing permissions, reviewing regularly, updating and removing permissions as appropriate.

8.5. Only share files with trusted sources.

9. Removable media

9.1. If storing or transferring personal, sensitive, confidential or classified information using Removable Media you must first contact IT Services for permission, but

9.1.1. Always consider if an alternative solution already exists;

9.1.2. Only use recommended removable media;

9.1.3. Encrypt and password protect;

9.1.4. Store all removable media securely;

9.1.5. Removable media must be disposed of securely by IT Services.

10. Personal use of ICT facilities

10.1.   Social media[1]

For the purposes of this policy, social media websites are web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. They include websites such as Facebook, Twitter, WhatsApp and LinkedIn. They also cover blogs and image sharing websites such as YouTube, Snapchat and Flickr. This is not an exhaustive list and you should be aware that this is a constantly changing area.

10.1.1. Use of Social Media at work

10.1.1.1.   Employees and volunteers are permitted to make reasonable and appropriate use of social media websites from the Trust's IT equipment. You should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to your non-working hours, unless this forms part of your work responsibilities.

10.1.1.2.   Access to particular social media websites may be withdrawn in the case of misuse.

10.1.1.3.   Inappropriate comments on social media websites can cause damage to the reputation of the Trust if a person is recognised as being an employee or volunteer. It is, therefore, imperative that you are respectful

---

[1] See also the Staff and Persons in a Position of Trust Code of Conduct

of the Trust's service as a whole including pupils, parents, colleagues, partners and other schools and academy trusts.

10.1.1.4. Employees and volunteers should not give the impression that they are representing, giving opinions or otherwise making statements on behalf of the Trust unless appropriately authorised to do so. Personal opinions must be acknowledged as such, and should not be represented in any way that might make them appear to be those of the Trust. Where appropriate, an explicit disclaimer should be included, for example: '*These statements and opinions are my own and not those of the Trust.*'

10.1.1.5. Any communications that employees or volunteers make in a personal capacity must not:

10.1.1.5.1. bring the Trust into disrepute, for example by criticising pupils, parents, colleagues or partner organisations;

10.1.1.5.2. breach the Trust's policy on confidentiality or any other relevant policy;

10.1.1.5.3. breach copyright, for example by using someone else's images or written content without permission;

10.1.1.5.4. do anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation;

10.1.1.5.5. use social media to bully another individual;

10.1.1.5.6. post images that are discriminatory or offensive (or links to such content).

10.1.2. The Trust maintains the right to monitor usage where there is suspicion of improper use.

10.2. Other personal use

10.2.1. Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls, playing computer games and browsing the internet) is permitted so long as such use does not:

10.2.1.1. incur specific expenditure for the Trust;

10.2.1.2. impact on the performance of your job or role (this is a matter between each employee or volunteer and their line manager);

10.2.1.3. break the law;

10.2.1.4. bring the Trust into disrepute;

10.2.1.5. detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos);

10.2.1.6. impact on the availability of resources needed (physical, network or cloud) for business use.

10.2.2. Any information contained within the Trust in any form is for use by the

employee or volunteer for the duration of their period of work and should not be used in any way other than for proper business purposes, or transferred into any other format (e.g. loaded onto a memory stick / pen drive), unless necessary for business use, and with prior agreement of your line manager and IT Services.

11. Portable and Mobile ICT Equipment

11.1. This section covers items such as laptops, mobile devices and removable data storage devices. Please refer to paragraph 9 of this document when considering storing or transferring personal or sensitive data.

11.2. Use of any portable and mobile ICT equipment must be authorised by IT Services before use.

11.3. All activities carried out on the Trust's systems and hardware will be monitored in accordance with the general policy.

11.4. Employees and volunteers must ensure that all data belonging to the Trust is stored on the Trust's network or cloud storage and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.

11.5. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.

11.6. Ensure automatic synchronisation of all locally stored data, including diary entries, with the appropriate cloud storage platform. If you are in doubt that this has been configured or is working effectively, please contact your local IT technician.

11.7. Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

11.8. The installation of any applications or software packages must be authorised by IT Services, fully licensed and only carried out by IT Services.

11.9. In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

11.10. Portable equipment must be transported in a protective case if one is supplied.

12. Wireless Access

12.1. The Trust supplies two different levels of wireless access; Trust Devices and Guest WiFi for BYOD (Bring Your Own Device).

12.2. Trust Devices is configured on trust owned devices by IT Services. This is setup by and authentication credentials are known only to IT Services. Devices connected via "Trust Mobile" wireless are treated exactly as a wired desktop PC and as such need to be protected.

12.3. Guest WiFi access is open to any wireless client. Clients connecting to Guest WiFi (BYOD) will either use the standard trust network login credentials, or credentials supplied by their home institution (if they participate in the Guest WiFi program).

12.4. By connecting to Guest WiFi (BYOD) users are agreeing to the terms of this document. It is the responsibility of the individual to ensure their device is free from viruses and any other malicious software.

12.5. BYOD has been limited to only allow access to internet and other web-based technologies (such as e-mail / VLE and other online information portals). Access to file shares (such as network drives) are not permitted and controls are in place to prevent it.

12.6. Users may access files and applications via the Trust's remote access facility. This is provided via a secure VDI (Virtual Desktop Infrastructure) system which is highly encrypted and secured.

13. Remote Access

13.1. If remote access is required, you must contact IT Services to set this up.

13.2. IT Services does not allow the connection of non-trust computer equipment to the network without prior written request and technical approval. This includes connection via web portals such as TeamViewer or Virtual Private Networking (VPN). This however excludes connecting devices via the Trust's BYOD (Bring Your Own Device) network.

13.3. You are responsible for all activity via your remote access facility.

13.4. Laptops and mobile devices must have appropriate access protection, i.e. passwords and encryption, and must not be left unattended in public places.

13.5. To prevent unauthorised access to the Trust's systems, keep all remote access information such as usernames, logon IDs and PINs confidential and do not disclose them to anyone.

13.6. Select PINs and passwords that are not easily guessed, e.g. do not use your house or telephone number and do not choose consecutive or repeated numbers.

13.7. Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

13.8. Protect the Trust's information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-office environment.

13.9. Users of laptops and mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged. Appropriate precautions should be taken to minimise risk of theft or damage.

13.10. Care should be taken when working on laptops in public places (e.g. trains) that any employee or pupil details are not visible to other people.

14. Remote learning

When delivering remote learning:

14.1. 1:1s should be avoided.

14.2. You should not behave any differently towards pupils compared with when they are in school. You must never attempt to arrange any meeting, including tutoring sessions, without the full prior knowledge and approval of the school, and should never do so directly with a pupil.

14.3. You should only use platforms specified by the school's SLT and approved by the Trust's Head of IT. You should not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.

14.4. Any live lessons should be recorded so that if any issues arise the video can be reviewed. The recording should be stored on the school's network in an area that can only be accessed by those staff who need to. It will be retained for a year, after which time it should be deleted. You must not take secret recordings or screenshots of yourself or pupils during live lessons.

14.5. You should conduct any video lessons in a professional manner, as if you were in school. This includes being suitably dressed, using professional and appropriate language and not being in a bedroom or bathroom. Where the use of a bedroom is unavoidable, it should be impossible to tell that it is a bedroom, even if the camera slips. The camera view should not include any personal information or inappropriate objects and where possible the background should be blurred/changed.

14.6. If anything inappropriate happens - or anything which could be construed in this way – you must immediately inform your line manager and keep a written record. This is for your protection as well as that of pupils.

14.7. You should look out for signs that a child may have been harmed or be at risk of harm, as you would if they were in school. Any concerns or disclosures must immediately be passed on to the Designated Safeguarding Lead or, in their absence, a deputy designated safeguarding lead, in line with the school's child protection procedures.

15. Electronic monitoring

15.1. You may find that you have access to electronic information about the activity of colleagues. Any such information must not be used by unauthorised individuals to monitor the activity of individual employees or volunteers in any way (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files, etc.) without their prior knowledge. Exceptions are:

15.1.1. In the case of a specific allegation of misconduct, when the safeguarding lead / investigating officer can authorise accessing of such information when investigating the allegation;

15.1.2. When IT Services cannot avoid accessing such information while fixing a problem, but this will only be carried out with the consent of the individual concerned.

16. Online purchasing

Any users who place and pay for orders online using personal details do so at their own risk and the Trust accepts no liability if details are fraudulently obtained whilst the user is using the Trust's equipment.

17. Care of equipment

17.1. Individual users are responsible for any trust equipment issued to them. Any damage or loss must be reported to IT Services as soon as it occurs, so that a repair can be made or a replacement issued. IT Services will keep a log, by user, of repairs and replacements.

17.2. Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling, modems etc.) without first contacting IT Services.

18. Related policies

This policy links with the following policies and procedures:

18.1. Disciplinary policy and procedure

18.2. Staff and persons in a position of trust code of conduct

18.3. Safeguarding policy

18.4. Child protection procedures

18.5. Photograph and video policy

18.6. Combined data protection and freedom of information policy

Appendix 1: Agreement

All employees, volunteers, contractors or temporary employees who have been granted the right to use the Trust's ICT systems are required to sign this agreement confirming they have read understood and accept the Trust's Acceptable Use of ICT Policy.

Employee/volunteer/contractor		Line Manager	
Name:		**Name:**	
Signed:		**Signed:**	
Date:		**Date:**	