COLLABORATIVE LEARNING TRUST

Working Together to Secure Success

COMPUTING FACILITIES GUIDANCE & ACCEPTABLE USE POLICY

Review date January 2025
Next Review January 2026

Table of Contents

Key Policy Points

- Do not install or move computer hardware
- Do not store data on the C drive of a school computer.
- Do not store sensitive data on the C drive of your staff laptop/ iPad unless it is encrypted
- Store data on OneDrive, your user area or shared drive as it is backed up
- Do not leave your laptop/iPad unattended
- Do not leave yourself logged in, always lock your desktop if you are leaving your computer/workstation unattended (Windows Key+L)
- Your laptop/-Pad is not insured if it is left unattended in a public, your car or an unlocked room
- Do not leave any login information in public view
- Always use a password at least 12 characters long; suggest adherence to the 3 unrelated words password regime
- Do not install any unlicensed software on any computer, laptop or iPad. Check with the CLT IT Support Team first
- Before purchasing hardware or software check with the CLT IT Support Team
- Do not plug any device other than your staff laptop/iPad into the network
- Do not attempt to access or modify any place or data on the network to which you are not authorised
- If wishing to use your own personal device (e.g. laptop, iPad) in school, adhere to the Bring Your Own Device Policy
- Never disclose any information about the school ICT facilities or personal data to anyone unless on school / Trust business and only where permitted within the provisions of the school's Data Protection Policy
- Take particular care to safeguard the security of personal data (e.g. MIS data)
- Do not store personal data on a USB memory stick unless it is encrypted
- Do not use personal equipment to record images of students, or to produce video or audio recordings of students, without prior permission from SLT
- Ensure that any electronic communication or publication does not contravene this policy
- Always check the conditions of use for any electronic material or web site
- Do not disable anti-virus software or attempt to circumvent antivirus measures in place within school
- Keep personal email and internet use to a minimum
- All access to the internet, logons to the network and file deletions are audited
- Any breach of this policy will be dealt with using the Trust's disciplinary policy

Introduction

The purpose of this document is to ensure that all members of staff (this includes all teaching and non-teaching staff) are aware of the policies relating to the use of all ICT facilities within the school / Trust, whether they are accessed within school or externally (this covers any access to or use of resources which reside within the school and any data relating to the school whether held within the school or externally).

This document covers school / Trust ICT facilities and all electronic information and data in use by or relating to the school with particular respect to email and internet security.

The ICT policy is in place to preserve:

- **Confidentiality**: Information is accessible only to those who are authorised to access it
- **Integrity**: Safeguarding the accuracy and completeness of information
- **Availability**: Ensuring authorised users have access to systems and information when required
- **Safeguarding**: maintaining safe learning and working environments for students and staff

It is the responsibility of all staff to read, understand and adhere to this policy. Staff members must also be aware of the ramifications of breaching this policy. Each member of staff will be required to sign a document confirming that they have read, understand and will keep up to date with the policy, and this will be held centrally by the school.

The policies herein do not in any way attempt to limit or prevent the use of the ICT facilities and data and are in place to protect the school and its staff from any misuse.

The Collaborative Learning Trust (CLT) actively encourages the use of ICT facilities within the school / Trust and is continually working to improve and extend ICT services for the benefit of teaching and learning alike. CLT wants to promote best practice and the responsible use of ICT facilities throughout the school.

Updates to this policy
Updates to the policy or supplements may be added and made available to staff either in paper or electronic format. Amendments must be adhered to and are agreed to by the act of signing the original document.

1. Computing Facilities

Access to all computing facilities is managed by the CLT IT Support Team. Any issues with the ICT facilities should be directed to this team; exception of All Saints Primary who have their own internal IT Support Team, in which case the internal IT Support Team should be made aware.

Definition
Computer facilities are defined as any piece of computer hardware or software that is either owned by the school / Trust or is owned by a member of staff and is in use on the business of school / Trust staff.

This is in order that any policies relating to the use of the network, internet, email or data on equipment owned by anyone other than the school / Trust is regulated within this document.

Ownership
All computing facilities within the school / Trust with the exception of equipment owned personally by staff members are the sole property of the school / Trust. Any change of ownership must be formally authorised by the governors and management team. Any work created by staff members in the course of their employment becomes the intellectual property of the employer under the Patents Act 1977 and the Copyright, Designs and Patents Act 1988.

Exchange of Assets
No department within school / Trust may exchange assets with any other body without the express permission of the management team.

Loss of or damage to assets
Accidental damage or theft of desktop computer assets will be covered under the school's insurance policy except for under the circumstances designated with * in this document.

1.1 Desktop Computers

Critical to the use of ICT for teaching and learning are the desktop PC's/Laptops which are in use throughout the school at each of the Trust Member sites. Maintaining the reliability, security and efficiency of these units is of paramount importance to the school / Trust.

1.1.1 Installation and configuration

No member of staff other than members of the CLT IT Support Team may install or reconfigure any hardware relating to the desktop computer. This does not include the insertion or removal of portable storage devices such as USB memory sticks although the use of such removable media is also discouraged; cloud storage i.e. OneDrive is recommended as a more comprehensive alternative.

In addition, if a member of staff should encounter a situation where the computer or any peripheral is unplugged and hence unusable then they may re-attach it. However, if there is any damage to the equipment or personal injury then the individual accepts all liability and the corresponding department may be asked to make financial reparations.

No member of staff other than members of the CLT IT Support Team must relocate, remove or dispose of any desktop computer.

This serves to protect the member of staff from any damage to the computer that might be caused or breach in the Health and Safety regulations.

1.1.2 Local Data

No personal or work-related data should be stored locally on any desktop computer within the school. Adequate provision for data storage is available on the school file servers along with Microsoft 365 Cloud Environment (OneDrive). This data is regularly backed up and is secure to prevent any data loss, corruption or misuse.

1.1.2.1 Exceptions

Some departments may have particular storage requirements which far exceed the capacity of the file servers and would be inefficient to store on a file server. For example, large digital video or audio files.

In the event that this information is stored locally then the head of the individual department takes responsibility for maintaining a backup of this data. The CLT IT Support Team will provide backup advice for staff members and in the event of a failure or loss will assist in attempting to recover the data.

However, neither the school, Trust or the CLT IT Support Team will be responsible for any inability to recover this data.

1.2 Portable Devices

Portable devices include laptops, iPads, smartphones etc are often specifically used by staff members. They are an essential tool for the success of the school and its staff as an

enabler for an on-time, anytime, anywhere information culture. They provide a significant boost to flexibility of ICT facilities for all staff. Portable devices are at significant risk from:

- Theft or accidental damage
- Data loss, theft, misuse or corruption - Data may be stored locally which is then potentially at risk from loss or corruption and especially theft or misuse as it is transported outside the school environment
- Security Attacks - vulnerability to virus and spyware attacks through virtue of being connected to the internet through ISP's other than the schools; potentially circumventing local filtering if not on school's WiFi network.

1.2.1 Rules governing portable devices

- Portable devices must not be left unattended in a non-secure environment such as an unlocked room*
- Portable devices must not be left unattended in a vehicle or public place*
- Portable devices may be left unattended in the staff member's place of residence
- The Trust strongly recommends that no-one other than a member of staff utilises a staff portable device e.g. family members
- The member of staff who is allocated the portable devices will be liable for any damage to it or any misuse of any data which is stored locally on the device
- The school or Trust will not be responsible for any unlicensed software which is installed on the portable device. The CLT IT Support Team will never install unlicensed software on such devices. However, staff members are allowed to install licensed or freeware software on the portable devices

1.2.2 Local Data

- No sensitive data in relation to the business of the school or students, should be stored locally on the portable device
- The school or Trust will not be liable for loss, corruption or misuse of any data stored locally on the portable devices. Liability rests with the individual to which the device is allocated
- The school or Trust will not be responsible for recovering any data which is stored locally and either corrupted or lost, however, we will endeavour to recover it to the best of our ability

Local data can be protected through the use of encryption. If any member of staff has a requirement to store sensitive data locally then they need to seek assistance from a member of the CLT IT Support Team on how to encrypt this data.

1.3 Peripherals

- No peripheral device may be installed or physically reconfigured by a member of staff
- If a peripheral device has become disconnected then the member of staff may reconnect it at their own risk and liability
- No peripheral should be permanently removed, disposed of or swapped without the direct approval of the CLT IT Support Team
- No purchase of peripherals should be undertaken without prior consultation with a member of the CLT IT Support Team. This tries to ensure that any peripheral will be compatible with the school's equipment and that the peripheral is fit for purpose.

1.3.1 Exceptions

If a department has a member of staff whose role or part role is to manage the department's ICT facilities then they may purchase and install peripheral devices. Neither

the school, Trust or CLT IT Support Team will take any responsibility for the failure of this device to meet the functional requirements of the department unless it is deemed to be a configuration fault of the core ICT systems or computer which the device is to be attached.

The CLT IT Support Team will enable the equipment to function if it deems the required configuration changes DO NOT cause a breach of the internal systems security.

1.4 Software

- Software may not be installed on any desktop PC within school by any member of staff except members of the CLT IT Support Team
- Software may be installed on a portable device provided it is licensed, however it is preferred for this to be centrally controlled and managed by CLT IT Support Team using Mobile Device Management (MDM).
- The purchase of software should not be made without consultation with the CLT IT Support Team
- The CLT IT Support Team will install software for the member of staff or department within the confines of the license agreement
- The member of staff or department is required to provide proof of the license agreement even if it is freeware
- The CLT IT Support Team will not break the license agreement and install the software in an inappropriate manner
- If any member of staff discovers software on a desktop or portable device which he/she feels is not licensed then they should alert the CLT IT Support Team immediately
- Any unlicensed use of software is illegal and any illegal use may be reported to the Federation Against Software Theft (FAST)
- Software must not be duplicated or distributed outside the scope of its licence agreement

Applications used for file sharing, such as Peer-to-Peer (P2P) or BitTorrent (or derivatives thereof), must not be installed on any PC or portable device as it poses a significant security threat and may be used to download illegal software and copyright protected works. If any such software is noticed on any Trust device, this must be brought to the attention of a member of CLT IT Support Team.

1.5 Cloud Services

Cloud Services are defined as any system, which stores data externally to the school's network. This includes virtual learning environments (VLE), email system, online storage systems and most sites that require you or students to log in via a website.

Staff must not store any sensitive data relating to the school or students on any cloud service not vetted by the school.

1.5.1 Approved Cloud Services

Staff may only use online / cloud services which have been approved by the school for the purposes of Data Protection, as listed in the school's Privacy Notices (see school website). If you want to use an online service other than those listed you must obtain permission. Should you require such permission then please speak to CLT IT Support Team in the first instance.

2. Network Access

Each school provides both wired and wireless network access across the majority of the site for the flexibility of staff and students alike.

Any intrusion to the network or connection of a rogue (unknown) device must not happen as this presents a significant security, functionality and performance risk.

2.1 Network access rules

- No devices should ever be plugged into a network point unless they are owned by the school / Trust or have been directly authorised for use on the school's network by the CLT IT Support Team.
- No network cables may be removed or plugged in to any device other than to attach a portable device to the network. Only, either under the supervision of CLT IT Support Team or directly/indirectly via CLT IT Support Team should any network cables be moved, removed or plugged in.
- You must not attempt to gain access to any areas of the school network to which you do not have access.
- If you feel that you have accidentally accessed an area of the network that you think you should not be able to access you must alert the CLT IT Support Team immediately.
- You must not attempt to install or use any network monitoring or packet sniffing software.
- You must not knowingly introduce a virus or carry out any hacking activities.
- You must not store on the network and then use any material which is protected by copyright, outside of the legal use parameters or any explicit usage rules of the work.

Breach of any or several of these points would mean that you had not only broken the Computing Facilities & Guidance Policy but also contravened the Computer Misuse Act 1990 which states that the following are offences:

- Unauthorised access to computer material e.g. Hacking
- Unauthorised modification of computer material
- Unauthorised access with intent to commit or facilitate the commission of further offences

2.2 Wireless access

All wireless data is secured via advanced authentication and encryption systems and therefore in the most part is secure.

Staff are expected to treat WiFi access with the same diligence, importance and consideration as physical network connectivity. Any personal devices automatically fall within the scope of associated BYOD policies and usage is expected to be kept to a minimum.

2.2.1 Wireless access rules in addition to wired rules

- No member of staff should attempt to move or reconfigure a wireless network access point.
- No member of staff should add/remove a wireless network access point to the existing wired network, wireless access points should only be administered by a member of CLT IT Support Team.

3. Other use of ICT Facilities

- ICT facilities must not be used for any business purposes other than those of the school / Trust.
- Configuration information about ICT systems must not be disclosed to anyone who is not a direct employee of the Trust, should such information be requested by a 3rd party, then this should be raised to a member of CLT IT Support Team.

4. Data Security

By far the most valuable asset within ICT is the data held on the ICT systems. Data does not just comprise files but also information within the school's management information systems (MIS) – namely Arbor for the majority or the Trust Member Sites, user account information and a wide variety of information stored in other systems. All this data must be protected and safeguarded and users only allowed to access information which they are authorised to do so.

All information stored on a school / Trust system, whether it be locally or hosted within a cloud environment, is backed up regularly to ensure its safety.

All data is held and disclosed within the bounds of the Data Protection Act. Personal data is held in accordance with the following data protection principles.

Personal data will be:

- Obtained and processed fairly and lawfully
- Held for specific lawful purpose(s)
- Not held or disclosed in a way incompatible with the purpose(s)
- Adequate, relevant and not excessive for the purpose
- Accurate and up to date
- Not kept longer than necessary
- Available to the data subject
- Kept secure

All data and correspondence, including email messages, held by the school / Trust may be provided to the data subject, internal or external, in the event of a subject access request.

4.1 Rules governing use of data

In order to maintain the security, integrity and accuracy of data the following rules will apply in conjunction with those outlined in the Data Protection Act:

You must not:

- Divulge personal information about any individual to another individual other than the data owner unless for the specific purpose of school / Trust business, and only where this is permitted within the provisions of the school's Data Protection Policy.
- Disclose any access credentials (i.e. usernames and passwords) for any ICT systems to anyone.
- Fail to maintain a paper or electronic copy of any credential information in either a public or insecure place which is accessible to others.
- Leave a computer workstation (desktop or portable) logged on and unattended.
- Usage of USB storage devices of any sort – no longer required as OneDrive has replaced this as a strongly recommended method of best practice.

- Print sensitive information and not collect it from a printer. If you think that the printer has not printed or that the print out has been removed you should contact a member of the CLT IT Support Team / SLT immediately.
- Give another member your password if at all possible either verbally, in written form or electronically.
- Allow anyone else to masquerade as you. This means that whilst you are logged on to the computer network or the internet no-one else is allowed to perform acts on the system as if they were you.

You must:

- Always lock your computer when you leave it unattended for short time period and intend to return, or if you are the sole user of the computer for any period of time when you are away from your desk. Only you or an administrator may unlock the computer.
- Always log out of the computer completely if you do not intend to return to it within a reasonable timescale where another user may require the use of the computer; simply staying logged on and locking the terminal is NOT satisfactory.
- Use a secure file sharing solution to transfer personal data in preference to a USB memory stick, e.g. 'wetransfer.com' wherever possible as this is inherently encrypted; USB devices should NOT be used if at all possible.
- Shred any hardcopies of sensitive information which you are not going to retain.

4.2 Password Policy

In line with the most recent guidance issued by the Information Commissioner's Office, the emphasis should be on making passwords difficult or complex to begin with rather than requiring frequent changes. The National Cyber Security Centre recommends that passwords contain three random unrelated words. Therefore, the password chosen:

- Must include three random, unrelated words (e.g. penciltrainfish but NOT sequential, e.g twothreefour).NOTE: Primaries are currently NOT in adherence to this policy until the new Password regime has been fully rolled out; expected 2023.
- Must be at least 12 characters long.
- *May* include a mixture of uppercase and lowercase letters, numbers, and special characters (e.g. PencilTrainFish3?).
- Must not be identical or substantially similar to any previous passwords.
- Must not be related to one's job or personal life (e.g. a spouse's name or fragments of an address).
- Must be committed to memory and not written down.
- Should only be changed when there is a data breach, or whenever a member of staff suspects that a password has become known to another person (compromised).

4.3 Auditing Policy

The following ICT audit policy is in place:

- All logons whether successful or failed are logged. Information about the time and location of these logon attempts is recorded.
- All file deletions from the servers whether successful or failed are logged. The time of deletion and the user account used to perform the deletion are logged.
- Retention is based on file size so no accurate retention time can be given.

4.4 Anti-Virus

The protection anti-virus software provides is essential to the correct functioning of the computer and the integrity of its data.

Every server, desktop and portable device is installed and configured with the Sophos Anti-Virus product. Updates to this software are automatic when connected to the internet, regardless of locality.

You must not:

- Attempt to remove, disable or circumvent the Sophos anti-virus software or remote update client from any computer.
- Install additional anti-virus software on any computer.
- Install any other anti-virus software on your staff laptop.

All staff portable devices update automatically via an internet connection regardless of locality. If, for any reason, you think that the anti-virus software is not functioning, updating or is not installed then please see a member of the CLT IT Support Team immediately and do not attach the computer to the network.

4.5 Anti-Spyware

You may not install any security software without the prior approval of the CLT IT Support Team; this includes anti-spyware software, anti-malware software or other security prevention software. Installing other security software could have a detrimental effect on the Sophos provision.

4.6 Firewalls

Firewalls prevent any network-based attacks on your computer by blocking communication on non-critical channels. All devices with Sophos installed will use the Firewall policies and technologies within Sophos InterceptX. Should a device NOT have Sophos installed then it will, by default, have 'limited' protection supplied by Windows Firewall.

You must not:

- Attempt to disable, remove or circumvent Sophos InterceptX in any way. Likewise, if Sophos InterceptX is NOT installed, you must not attempt to remove,disable or circumvent Windows Firewall. Notify or alert a member of the Trust ICT Team.
- Install any other firewall software e.g. Zone Alarm, McAfee etc as this may interfere with the ability of your laptop to connect correctly to the school network and will most likely result in performance degradation of the device.

We appreciate that some Internet Service Providers (ISP's) install firewalls automatically. Whilst this is 'unlikely', if you think that you have another firewall installed and are having difficulty connecting to your school's network please see a member of the CLT IT Support Team.

4.7 Access to the MIS database

Particular care must be taken to maintain and safeguard the security of personal data stored within the school's main management information system – namely Arbor with the Trust Member sites. By its very nature, much of this information constitutes what is known as "sensitive personal data", which is subject to stringent additional restrictions within data privacy law.

In particular, personal data contained within the MIS:

- Must only be shared in accordance with the Data Protection Policy.

- Must not be printed, except where this is unavoidable (e.g. to provide Progress Reports for parents/carers)
- Must not be transferred to a remote device (except in exceptional circumstances where appropriate security measures are implemented – e.g. encryption)

Staff should only log into the MIS when there is a specific purpose for doing so (e.g. to register students), and must log out again as soon as access is no longer required.

5. Email and Internet

Any electronic communication or publication may be accessed and checked by the Headteacher or CEO should the need arise.

Guidance regarding best practice and E-Safety is available in Section 8.

5.1 Email

Each member of staff is provided with an email account through school and is expected to check their email regularly – at least twice a day.

Users may access their email through the Outlook Email client in school or at home, or via a web browser.

You may also access Outlook Web Access within school via the homepage.

Inappropriate use of email can expose the school or Trust to significant liability for example copyright and trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements.

School-wide messages must be business related and be of significant importance to the majority of staff members.

5.1.1 Content

- Email messages must be treated as formal written communication.
- Email messages cannot be considered as private, secure or temporary.
- You have to assume that an email could be read by anyone
- Improper statements can lead to personal or school / Trust liability. Emails could misrepresent or give an unfavourable impression of the school or Trust, its business, employee, suppliers or anybody linked to the school or Trust.
- Do not create or send emails which are, or could be construed as, defamatory or derogatory.
- If it is absolutely necessary to send sensitive personal data via email, this must be encrypted / password protected (attachments) then the password sent by other means in a separate transmission; encryption is achievable via the use of inbuilt functionality within Microsoft Outlook. Whilst files can be sent securely via the 'wetransfer.com' platform as this is inherently encrypted, it is strongly advised that you utilise the recipient's own platform to facilitate this wherever possible, e.g. Local Authority's secure file transfer protocol.
- Do not create emails which are intimidating, hostile or offensive in any way.
- Copyright law also applies to emails.

5.1.2 Privacy

Email messages to and from you cannot be considered private and confidential.

When sending emails to groups of people outside the school /Trust, you must always use the blind carbon copy facility (Bcc).

It is not acceptable to send or receive email to/from an email account which is not your own without the express permission of that individual. The prior rules on disclosure of credentials also apply to email accounts.

5.1.3 Security

The school / Trust scans email for viruses and filters the majority of spam. However, as users we have a responsibility to remain vigilant and follow these guidelines:

- Never open an email and/or and attachment from an unsolicited source
- Never open an attachment from an unsolicited source or from a trusted source if it seems in anyway suspicious or non-work related
- Never follow links in emails that you were not expecting If you are unsure seek advice from the CLT IT Support Team.

5.2 Internet usage

The following basic principles and rules have been developed and staff wishing to have internet access will be expected to adhere to these.

1. The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management
2. All Internet use should be appropriate to staff professional activity or students' education. Legitimate private interests may be followed, providing school use is not compromised (such interests include private research, work for examination boards, research for courses)
3. Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed. The downloading of inappropriate sexist, racist, pornographic, indecent, violent or abusive images, text or sound files is forbidden
4. Access must only be made via the authorised account and password, which must not be made available to any other person
5. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited
6. The downloading of any program, screen saver, game etc without permission from the Headteacher or CLT IT Support Team is forbidden
7. Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden
8. Permission must be sought from students and parents before any personal data, i.e. names and photographs are published on an external web site
9. Users are responsible for e-mail they send and for contacts made that may result in e-mail being received
10. The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded
11. The sending of sensitive personal data must be in strict accordance with the school's Data Protection Policy.
12. The sending of any information which is not certain to be 'public knowledge' outside the school is forbidden
13. Posting anonymous messages and forwarding chain letters is forbidden
14. Copyright of materials and intellectual property rights must be respected
15. No unauthorised contract, purchase or payment should be made over the Internet

16. Use for personal financial gain, gambling, political purposes or advertising is forbidden
17. The school or Trust will not be liable under any circumstances for any injury, distress, loss or damage to staff, students or parents, which may arise directly or indirectly from the use of the Internet facilities, the use of e-mail, or from other persons' unauthorised use of those facilities or e-mail

5.2.1 Web Publishing

Documents published to the web must not:

- Be defamatory
- Be intimidating, hostile or offensive under any circumstances
- Be discriminating in any way
- Diminish the reputation or image of the school / Trust
- Infringe copyright of the author
- Be of a sensitive nature unless access to the documents is controlled through a specific access control mechanism which limits access to the appropriate audience, and is permitted within the provisions of the Trust's Data Protection Policy.

5.2.2 Viewing or downloading documents or files

The same rules apply to the viewing or downloading of documents, plus:

- You must comply with the terms and conditions governing a website's use when you access it.
- Access to some websites is blocked by the school / Trust. If you have a genuine reason to access a blocked website please see a member of the CLT IT Support Team.

5.2.2.1 Exceptions

If any electronic resource features content of a nature listed in 5.2.1 (Points 1, 2, 3) but is in the interest of teaching and learning, then it may be used. However, use of the content must not breach 5.2.1 (Points 4, 5, 6, 7) or intend to promote any illegal acts or discriminatory attitudes.

5.3 Newsgroups and discussion boards

Posting to newsgroups comes under the same rules as the use of email and web publishing which are described in the previous section.

No member of staff may set up a newsgroup in which to solicit information about people's opinions of the school, Trust or its staff without the prior approval of a member of the SLT.

5.4 Web Logs

Web logs or blogs fall under the same rules governing email and web publishing. Publishing personal opinions with regards to the school or Trust is not advised.

5.5 Instant Messaging

Instant messaging can be a useful tool for real-time communication. It must be used solely for a professional reason.

In the event that Instant Messaging is being used then the same policy governing the use of Email applies.

The school / Trust does not enable the Microsoft messaging clients (Windows or MSN) and would discourage staff from installing or using these or any other instant messaging client on their portable devices.

5.6 Personal Use

Personal use of email or the internet is permitted but you must abide by the rules concerning content that are outlined above. Personal email or internet use must be kept to a minimum such that it does not interfere with the performance of your duties.

5.7 Monitoring and Auditing

All visits to web sites with information about the URL (Address) visited, username and time are logged. The school / Trust has the ability to examine these logs and any complaint relating to use of the web will be investigated.

6 Discipline Procedure

Any breach of this policy by a member of staff will be dealt with under the Trust's standard disciplinary procedures.

7 Ownership

7.1 Ownership

All devices and all related software and hardware remains property of the school / Trust

7.2 Return

All devices must be returned on request to the school / Trust within 72 hours of Request.

Devices must be returned with all related accessories, cables and packaging in a good working order as was given to you. If any of the items are not returned or are not deemed to be in a good working order you are liable to pay the cost to repair or replace them

8. Guidance regarding best practice and E-Safety

Introduction

The aim of this guidance is to inform all staff of best practice around E Safety and draw attention to existing local and national guidance on this subject. It is our responsibility to safeguard young people and protect staff from false accusations of improper conduct so that together we can ultimately maintain the safest possible learning and working environments for children and staff alike.

This guidance is in line with national guidance issued by the Department for Education as well as also drawing information from existing policies issued by Leeds Safeguarding Children Board and Leeds City Council.

Whilst care has been taken to consider all aspects of E Safety there may be times when members of staff, schools and services need to make independent judgments on individual situations not covered in this document. It is expected that in these circumstances that all staff will advise their senior colleagues of such action taken or proposed and schools will seek further advice from HR.

This document applies to all members of staff employed either directly or indirectly by the Trust or Member Schools. All members of staff are expected to adhere to this code of practice to ensure the safety of the young people in their care and in doing so fully abide by the guidance contained herein. Any member of staff found to be in breach of these guidelines may be subject to disciplinary action.

For the purpose of this document 'Students', 'Children' and 'Young People' will refer to all children and young people who members of staff have contact with as part of their professional capacity and to which all staff have a professional duty of care.

For the purpose of this document 'Schools', 'Services' and 'Organisations' will refer to the employer and place of work of all members of staff, whether the place of work is permanent, temporary or peripatetic.

8.1 Social Contact with Students, Children or Young People

8.1.1
Staff must not establish or seek to establish social contact with students, children or young people for the purpose of securing a friendship or to pursue or strengthen a relationship. Even if a student, child or young person seeks to establish social contact, or if this occurs coincidentally, the member of staff should exercise his or her professional judgement in making a response and be aware that such social contact could be misconstrued.

8.1.2
All contact with students, children or young people should be through appropriate channels at all times. Any communication outside of agreed professional boundaries could be prone to misinterpretation and as a result could put both the employee and young person at risk.

8.1.3
Staff should not give, nor be required to give, their personal details such as home or mobile phone number, Instant Messenger identities or personal e-mail address to students, children or young people. Staff should not use any of the above means to contact students, children or young people without the prior and explicit consent of Senior Leadership. Any member of staff found to be in contact with students, children or young people through any of the above means, or any other unapproved method, without prior consent could be subject to disciplinary action.

8.1.4
Internal e-mail and approved contact systems should only be used in accordance with the appropriate Trust, school or service Information Security Policy.

8.1.5
This means that members of staff should:

- always seek approval from Senior Leadership for any planned social contact with students, children or young people for example when it is part of a reward scheme or pastoral care programme
- advise Senior Leadership of any regular social contact they have with a student, child or young person which may give rise to concern
- report and record any situation which they feel might compromise the reputation of the organisation or their own professional standing

8.2 Social Networking Websites

8.2.1
Members of staff must not have any contact with students, children or young people through such sites and staff must not add students, children or young people as friends or respond to requests for friendship from children if asked. If a member of staff suspects that an existing friend is a student, child or young person, they should take reasonable steps to check the identity of the individual and end the friendship should the suspicions not be put to rest.

8.2.2
It is recognised that personal access to Social Networking sites outside the work environment is at the discretion of the individual however members of staff should consider their use of social networks as they take on the responsibilities of a professional, taking particular care to secure personal information and ensure their use of such networking sites is respectable and appropriate at all times.

8.2.3
Secure and suitable strength passwords should be devised and security settings should be applied so access to your profile and the information contained is limited to those explicitly given access.

8.2.4
Personal profiles on social networking sites and other internet posting forums must not identify your employer or place of work and careful consideration should be given to information which is published on such sites. For example, information which is confidential or could put others at risk should not be posted on such public domains. If the material you post or display is considered inappropriate or could be considered to bring your Trust, a Member School or profession into disrepute, disciplinary action may be considered.

8.2.5
Staff wishing to use Social Media within the context of their employment must gain authorisation to do so in accordance with the Policy on the Use of Social Media (on behalf of the Trust or school). The member of staff remains responsible for the content and monitoring thereof.

8.3 Inappropriate Material

8.3.1
When considering what is defined as inappropriate material it is important to differentiate between inappropriate and illegal and inappropriate but legal. All staff should be aware that in the former, case investigation may lead to criminal investigation, prosecution dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

8.3.2 Illegal Material

It is illegal to possess or distribute indecent images of a person under 18 and viewing such images on-line may constitute possession even if not saved. Accessing child pornography or indecent images of children on the internet, and making, storing or disseminating such material is illegal and if proven will invariably lead to the individual being barred from work with children and young people.

8.3.3 Material which incites hate, harm or harassment

There are a range of offences in relation to incitement of hatred on the basis of race, religion, sexual orientation and particular offences concerning harassing or threatening individuals which includes cyber bullying by mobile phone and social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

8.3.4 Professionally Inappropriate Material

Actions outside the work place that could be considered so serious as to fundamentally breach the trust and confidence in the employee may constitute Gross Misconduct. These actions may not always be illegal. For example, using work equipment to access inappropriate or indecent material, including 'adult pornography', will give the school or service rightful cause for concern particularly if as a result children or young people might be exposed to inappropriate or indecent material. Such behaviour would be considered inappropriate and could result in disciplinary action.

Some examples of inappropriate material and actions are:

- Posting offensive or insulting comments about colleagues on social media or networking sites;
- Accessing adult pornography on work based computers during break;
- Making derogatory comments about students or colleagues on social networking sites;
- Posting unprofessional comments about ones profession or workplace on social networking sites.
- Making inappropriate statements or asking inappropriate questions about students on social networking sites.
- Contacting students by email or social networking without senior staff approval.
- Trading in fetish equipment or adult pornography.

8.4 Creating images or video / audio recordings of students

8.4.1

Many work-based activities involve recording images and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. However, this must be undertaken in strict accordance with this policy, taking account of the specific points below in particular.

8.4.2

Using images / recordings of children for publicity purposes requires the age-appropriate consent of the individual concerned and their legal guardians. Images / recordings should not be displayed on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the school or service provision have access.

8.4.3

Photograph(s) or video images must be created using equipment provided by the work place. It is not acceptable to record images / video / audio of children on personal equipment such as personal cameras, mobile phones, video cameras or other electronic computer devices without prior consent from SLT. Images / recordings of children must not be created or stored for personal use.

8.4.4
Members of staff creating or storing images / recordings of children using personal equipment without prior consent may be subject to disciplinary action.

8.4.5
Members of staff must:

- be clear about the purpose of the activity and about what will happen to the photographs / recordings when the lesson / activity is concluded
- ensure that all images / recordings are available for scrutiny in order to screen for acceptability
- be able to justify images / recordings of children in their possession
- avoid making images / recordings in one to one situations (except where specifically permitted e.g. MFL speaking exams)

8.4.6
Members of staff must not distribute images / recordings of children unless they have consent to do so. Failure to follow any part of this code of practice could result in disciplinary action being taken.

8.5 Internet Use

8.5.1
Members of staff must follow and adhere to the policies on the use of IT equipment at all times and must not share logins or password information with other members of staff, students, children or young people, friends, family or members of the public.

8.5.2
Under no circumstances should members of staff in the work place access inappropriate images using either personal or work based equipment. Accessing child pornography or indecent images of children on the internet, and making, storing or disseminating such material is illegal and if proven will invariably lead to disciplinary action the individual being barred from work with children and young people.

8.5.3
Staff will NOT use work-based equipment to access inappropriate or indecent material, including adult pornography, either in the workplace or at home. This could result in disciplinary action.

8.6 Use of personal technology/equipment in school (Bring Your Own Device Policy)

8.6.1
The use of any personal equipment in school (e.g. personal laptops, iPads) must comply with this Computing Facilities Guidance & Acceptable Use Policy as well as Health & Safety regulations and the Data Protection Policy. Any member of staff found to be using such personal equipment in a way which contravenes these policies / regulations may be subject to disciplinary action.

8.6.2
Personal equipment must not be used for recording images, videos or sounds without prior permission from SLT.

8.6.3
Personal devices must be password protected or, preferably, secured by a biometric access control (e.g. fingerprint scanner or facial recognition). Passwords applied to a personal device must be kept confidential. When not directly in use, devices must be locked to prevent any unauthorised access.

8.6.4
Personal devices should not be used in a manner which puts at risk confidential information and personal data connected to the school e.g. by accessing links in suspicious emails or using potentially harmful applications. Personal devices, particularly laptops, must be installed with appropriate anti-virus software.

8.6.5
In the event that a personal device is lost or stolen, the member of staff must inform CLT IT Support Team immediately and ensure that their password is changed. In the case of mobile phones and tablets, the member of staff must also immediately contact the relevant network provider to block the device.

8.6.6
In the event that a personal device is to be disposed of or sold, the member of staff must ensure that all school-related information is wiped from the device. In the case of an iPad, this includes performing a full reset by selecting 'Erase All Content and Settings'.

8.7 Propriety and Behaviour

8.7.1
All members of staff have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children and young people. They should adopt high standards of personal conduct in order to maintain the confidence and respect of their peers, children and the public in general.

8.7.2
Members of staff should not behave in a manner which would lead any reasonable person to question their suitability to work with children or act as a role model. This includes behaviour in virtual online communities as well day to day social situations. Members of Staff also should not make (or encourage others to make) unprofessional personal comments through online media which scapegoat demean or humiliate, or might be interpreted as such.

8.7.3
An individual's behaviour, either in or out of the workplace, should not compromise his or her position within the work setting nor bring the Trust, school or organisation into disrepute.

8.7.4
If an allegation is received that a member of staff is responsible for comments made (online or otherwise) which could be deemed harmful, threatening, defamatory or abusive to the Trust, school or organisation, this will be investigated using the appropriate procedure. Any actions which bring the organisation or profession into disrepute will be considered under the appropriate policy and appropriate action taken in line with that procedure.

8.8 Confidentiality

8.8.1
Members of staff may have access to confidential information about students, children or young people and the organisation in order to undertake their everyday responsibilities and in some circumstances this may be highly sensitive or private information. Such information should never be shared with anyone outside the Trust, school, a member of the public or outside agencies, except in specific circumstances, for example when abuse is alleged or suspected. In such cases, individuals have a duty to pass information on without delay, but only to those with designated child protection responsibilities or a senior member of staff.

8.8.2
Care should be taken with the storage of such confidential information. Confidential information should never be stored on personal computers or devices or distributed through personal email or internet channels. Only authorised Trust, school-based devices and systems should be used to store and transfer confidential information. Members of Staff found to be compromising confidentiality by use of unauthorised systems and devices could be subject to disciplinary action.

8.8.3
The storing and processing of personal information about students is governed by the Data Protection Act 2018.

8.9 Cyberbullying

8.9.1
All forms of bullying, including cyberbullying, are taken very seriously. Bullying is never tolerated and it is not acceptable for any member of staff to behave in a manner which is intimidating, threatening or in any way discriminatory. Behaviour which constitutes Bullying or Harassment may be dealt with under the Bullying and Harassment Policy and could result in disciplinary action.

8.9.2
However, this doesn't just extend to behaviour within the work place. In some instances bullying or harassment that occurs outside the workplace, where there is a link to employment, could also fall under the responsibility of the employer and therefore result in disciplinary action being taken against the responsible individual.

8.9.3
Certain activities relating to cyberbullying could be considered criminal offences under a range of different laws. Cyberbullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice based bullying or discrimination through a variety of media. Media used could include email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

8.9.4
If an allegation is received that a member of staff is responsible for comments made online which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another employee, the Trust / organisation will investigate this matter. Any allegation of Bullying or Harassment made by an employee against another member of staff where the accused uses the internet, mobile phone, text message or email, along with any other forms of abuse, may be dealt with through the Bullying and Harassment policy and could lead to disciplinary action.

8.9.5
Staff are required to take steps to protect themselves and their personal information by:

- Keeping all passwords secret and protect access to their online accounts
- Not befriending children and young people on social networking services and sites
- Keeping personal phone numbers private
- Not using personal phones to contact parents and students, children and young people
- Keeping personal phones secure, i.e. through use of a pin code, when within work
- Not posting information about themselves that they wouldn't want employers colleagues, students, children, young people or parents to see
- Not retaliating to any incident
- Keeping evidence of any incident
- Promptly reporting any incident using existing routes for reporting concerns.

8.9.6
Any incident of cyberbullying will be investigated under the appropriate policy and could result in disciplinary action.

Further information and advice regarding the above issues can be found in:
LSCB E Safety Guide 2009/2010 version 2.0 Safe Working Practice Policy
DfE guidance document Cyberbullying – Supporting School Staff

and on the Trust's / Member school's dashboard under Policies:
Safe Working Practice
Keeping Children Safe in Education
Safeguard & Child Protection