



Castleford Academy Trust

Information and Communication Technology Acceptable Use Policy

Version No:	Date Ratified:	Review Date:
1.0	15/05/2024	15/05/2027



Contents

1. Introduction	3
2. Scope	3
3. Updates to this policy	3
4. Privacy	3
5. Section One – General policy and code of practice	4
6. Section Two – Internet policy and code of practice	9
7. Section Three – E-mail policy and code of practice	12
7.1. E-mail Policy – advice to staff.....	14
8. Section Four – Social media use and code of practice	15
9. Appendix 1 – Live Lessons – Staff Protocol.....	16



1. Introduction

Castleford Academy Trust IT acceptable use policy is divided into the following four sections.

1. General policy and code of practice
2. Internet policy and code of practice
3. E-mail policy and code of practice
4. Social media use

This document covers Castleford Academy Trust ICT facilities and all electronic information and data in use by or relating to the Trust with particular respect to email and internet security. The same policies and guidance apply when accessing Castleford Academy Trust systems remotely.

2. Scope

The policy covers:

- All employees of Castleford Academy Trust;
- All voluntary workers that are given access to the use of computer equipment;
- Trainee teachers and work experience pupils;
- Third party users such as supply staff / LA staff;
- Pupils, parents, trustees and governors (where applicable);
- All hardware and software purchased by the Trust for use by the above user groups.

Castleford Academy Trust actively encourages the use of ICT facilities within the Trust and is continually working to improve and extend ICT services for the benefit of teaching and learning alike. Castleford Academy Trust wants to promote best practice and responsible use of ICT facilities throughout the Trust.

This policy has been written in line with the most up to date version of Keeping Children Safe in Education.

3. 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.

4. Privacy

In particular please note the provisions set out in this ICT policy about privacy and how the Trust may monitor data, information and material in relation to or used, sent or received by staff.



5. Section One – General policy and code of practice

The Trust has well-developed and advanced ICT systems, which it intends to be useful and beneficial to all staff and pupils. This policy sets out the rules that staff must comply with to ensure that the system works effectively for everyone.

Privacy

The Trust will respect staff privacy however, in order to protect pupils' safety and well-being and to protect the Trust from any third-party claims or legal action, the Trust may view any data, information or material on the Trust's ICT system (whether contained in an e-mail, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services.

The Trust disclaimer which automatically appears at the end of each of e-mails notifies the recipient that any e-mail correspondence may be monitored. Staff must not remove this disclaimer. Staff should bring to the attention of any person who wishes or intends to send you an e-mail that the content of the email may be monitored.

Staff should never disclose information about the Trust ICT facilities or personal data to anyone unless on Castleford Academy Trust business.

The storage and processing of personal information about pupils is governed by GDPR, see the Trust's 'Data Protection Policy for further information.

All staff employed by the Trust are expected to undertake National Cyber Security Centre (NCSC) training as part of their induction.

Code of practice

Trust philosophy	In using ICT, staff will follow the Trust's ethos and consider the work and feelings of others. Staff must not use the system in a way that might cause annoyance or loss of service to other users.
Times of access	The network is available during term time. Out of term time the network will be subject to maintenance downtime and so may not be available for brief periods.



<p>User ID and password and logging on</p>	<p>Staff will be given a user ID and password. This must be kept secret and should not be shared with anyone.</p> <p>Passwords should be at least six characters long and a mixture of capitals, lower case letters, numbers and symbols. In the event that staff forget or accidentally disclose passwords to anyone else, this must reported immediately to a member of the ICT support staff.</p> <p>Staff must not use another person’s account or allow another person to use their account. The facilities are allocated to staff on a personal basis, staff are responsible for the use of the machine when they are logged on. Trust systems are used to record and monitor, the use of the system.</p> <p>Where staff share their username or password with a third party, any misuse by unauthorised users will be the responsibility of the staff member.</p> <p>Staff must lock their computer when it is left unattended.</p> <p>Castleford Academy Trust reserves the right to request staff to change their password.</p>
<p>Printing</p>	<p>The Trust may wish to check that expensive resources are being used efficiently and may share strategies with staff in order to save on resources.</p>
<p>Logging off</p>	<p>Staff must either lock or log off from the computer that they are using at the end of each session and wait for the standard login screen to reappear before leaving. This ensures security and frees up resources for others to use.</p>
<p>Access to information not normally available</p>	<p>Staff must not use the system or the internet in order to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. If staff feel that they have accidentally accessed an area of the network that they think should not be able to access, they must alert the ICT Network Manager immediately.</p> <p>Staff must not attempt to install software to explore or harm the system. Use of hacking tools e.g. ‘loggers’, ‘sniffers’ or ‘evidence elimination software’ is expressly forbidden.</p>
<p>Connections to the system</p>	<p>Staff must not connect any hardware which may be detrimental to the network.</p>



<p>Connections to the computer</p>	<p>Staff should use the keyboard, mouse and any headphones provided. Staff must not adjust or alter any settings or switches without first obtaining the written permission of a member of the ICT staff.</p> <p>Staff must never attempt to use any of the connectors on the back of any desktop computer. Staff may use USB memory stick ports, floppy disk and CD ROM drives, where provided on the front of the computers.</p> <p>Data on portable devices, such as USBs, must be encrypted as part of data protection guidance.</p> <p>Staff are not permitted to connect anything else to the computer without first getting the permission of a member of the ICT staff.</p>
<p>Portable Devices</p>	<p>Rules governing portable devices – including laptops, iPads and tablets</p> <ul style="list-style-type: none"> • 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 • No-one other than a member of Castleford Academy Trust staff may utilise a staff portable device e.g. family members. • Castleford Academy Trust will not be responsible for any unlicensed software which is installed on the portable device. The 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. • No sensitive data in relation to the business of the Trust should be stored locally on the portable device, in line with the UK GDPR. • If any user has a requirement to store sensitive data locally assistance should be sought from the IT support team to ensure this data is encrypted. • Staff must not plug any device other than staff equipment into the network as this presents a significant security, functionality and performance risk. • Confidential information should never be stored on personal computers or portable devices. Only authorised devices and systems should be used to store and transfer confidential information. • Members of staff found to be compromising confidentiality but use of unauthorised devices may be subject to disciplinary action. • Photographs or video images of pupils must only be created using equipment provided by the Trust. Members of staff creating or storing images of children using their personal equipment without prior consent may be subject to disciplinary action.
<p>Virus</p>	<p>Every server, desktop and portable device is installed with an Anti-Virus product. Updates to this software are automatic when connected the network.</p> <p>Staff must not knowingly introduce a virus or carry out any hacking activities. If staff suspect that a computer has a virus, they must report it to a member of the ICT staff immediately.</p>



	<p>If, for any reason, staff think that the anti-virus software is not functioning, updating or is not installed then they must see a member of the IT support team.</p> <p>Staff must not:</p> <ul style="list-style-type: none"> • Remove the 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 laptop.
Installation of software, files or media	<p>The purchase of software should not be made without consultation with the IT Support team.</p> <p>Staff (with the exception of the IT Support team) must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers. Staff must not alter or re-configure software on any part of the system.</p> <p>The IT Support team will install software for the user or department within the confines of the license agreement.</p> <p>If any user discovers software on a desktop or portable device which they feel is not licensed, they should alert the IT Support team immediately.</p> <p>Software must not be duplicated or distributed outside the scope of its license agreement.</p> <p>Applications used for P2P file sharing such as Kazaa or Bit Torrent, must not be installed on any PC or portable device.</p>
File space	<p>Staff must manage their own file space by deleting old data rigorously and by deleting emails that you no longer required. Where staff believe there is a real need for additional space, this should be discussed with a senior member of the ICT support staff.</p>
Transferring files	<p>You must not import or export any material unless the owner of that material expressly permits you to do so.</p> <p>Staff must always check the conditions of use for any electronic material or web site.</p>
Reporting faults and malfunctions	<p>Staff must report any faults or malfunctions in writing to the ICT support staff including full details and all error messages as soon as possible using the appropriate reporting tool.</p>
Food and drink	<p>Staff must not eat or drink nor bring food or drink, including sweets and chewing gum, into ICT rooms. Staff must maintain a clean and quiet working environment at all times.</p>
Copying and plagiarising	<p>Staff must not plagiarise or copy any material which does not belong to them.</p>



<p>Copies of important work</p>	<p>It is staff responsibility to keep paper copies and back-up copies on floppy disk, CD or memory stick or online of work and, in particular, staff must keep copies of any important work that you might have.</p> <p>Castleford Academy Trust will not be responsible for recovering any data which is stored either locally and either corrupted or lost, however will endeavour to recover it wherever possible.</p>
<p>Personal Use</p>	<p>Personal email or internet use must be kept to a minimum such that it does not interfere with the performance of staff duties.</p> <p>Legitimate private interests may be followed, providing Trust use is not compromised (such interests include private research, work for examination)</p> <p>Castleford Academy Trust ICT facilities must not be used for business purposes other than those of Castleford Academy. Castleford Academy Trust ICT systems must not be disclosed to anyone who is not a direct employee of Castleford Academy Trust.</p> <p>Use of Castleford Academy Trust equipment such as computers, phones and/ or tablets to access social networking sites for personal reasons is only acceptable before or after working hours or during break/ lunchtime.</p> <p>Any equipment provided to a member of staff is provided for their own personal use. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.</p>
<p>Wireless Access</p>	<p>Staff laptops are specifically configured not to allow a connection for anyone other than staff members or members of the IT support team.</p> <p>Wireless connections will not function in most cases when you are logged on locally i.e. logged on to the laptop and not logged on to the network. This is by design to prevent any security breach if a laptop is compromised or stolen.</p> <p>No user should attempt to move or reconfigure a wireless network access point.</p> <p>No user should add an additional wireless network access point to the existing wired network.</p> <p>No network cables may be removed or plugged into any device other than to attach a portable device to the network.</p>
<p>Loss or damage to assets</p>	<p>It is the user's responsibility to inform a member of SLT immediately if any computer facilities/hardware or portable devices including I-pads, laptops, phone or tablets become lost, damaged or stolen.</p> <p>After investigation, if the damage is a result of negligence, individual members of staff may be charged.</p>



<p>Ownership and Return of Property</p>	<p>All computing facilities within the Trust, with the exception of equipment owned personally by staff members, are the sole property of the Castleford Academy Trust. Any change of ownership must be formally authorised.</p> <p>All devices must be returned on request to Castleford Academy Trust. Devices must be returned with all related accessories, cables and packaging in good working order. If any items are not returned or are not deemed to be in a good working order, individuals are liable to pay the cost of replacement or repair.</p>
--	---

6. Section Two – Internet policy and code of practice

The Trust is able to provide access to the internet from desktop PC's via the computer network and through a variety of electronic devices connected wirelessly to the network. Whenever accessing the internet using the Trust, or personal equipment, staff must observe the code of practice set out below. This policy and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, staff or other pupils being offended and the Trust's facilities and information being damaged.

Consequently, any breach of this policy and the code of practice will be treated extremely seriously and it may result in disciplinary or legal action or expulsion. The Trust may take steps, including legal action where appropriate, to recover from an individual any expense or liabilities the Trust incurs as a result of the breach of this policy and code of practice.

Why is a code of practice necessary?

There are four main issues:

- Although the internet is often described as 'free', in fact there is a significant cost to the Trust for its use. This cost includes telephone line charges, subscription costs (which may depend on how much a service is used) and the computer hardware and software needed to support internet access.
- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. Using the internet effectively requires training and self-discipline. Training is available on request from ICT staff.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle, and to protect the Trust's staff and the pupils that access to this unregulated resource is properly managed by the Trust. Accessing certain websites and services and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of importing viruses on to the network, or passing viruses to a third party, via material downloaded from or received via the internet, or bought on-site on a USB or other storage media.

Filtering and Monitoring

- Some material available via the Internet is unsuitable for pupils. The Trust and, each academy within the Trust, will take all reasonable precautions to ensure such material is not accessed by pupils. However, it is not possible to guarantee that such material will never appear on a computer – Castleford Academy Trust cannot accept liability for material accessed or any consequences of Internet access.



- Castleford Academy Trust use Smoothwall as their filtering and monitoring tool. This is recommended by the UK safer internet council and the DFE.
- DSLs are responsible for filtering and monitoring across the Trust in their own settings. They will work with the IT network manager to ensure that sites are not over- blocked and checks are undertaken regularly.
- CPD is offered to senior DSLs in the trust to ensure that they have a working knowledge of Smoothwall.
- The Trust will work in partnership with parents, the DFE and the Internet Service Provider to ensure systems to protect pupils are regularly reviewed and improved.
- Any Internet user must report unsuitable/illegal sites to the Network Manager (and the Designated Safeguarding Lead if necessary) immediately. Alerts will be sent to the DSLs teams in each trust where an alert is triggered.
- The Network Manager will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable. Content is filtered using: Smoothwall and 'Fortigate' and communications are monitored through 'AB Tutor'.
- If filtered websites need to be used by staff, they must inform ICT Technicians to have them unblocked for a set period of time (requests need to be approved by the Line Manager).
- With regard to radicalisation via the internet and social media, Castleford Academy Trust fully adopts The Prevent Duty.

Code of practice

<p>Use of the internet</p>	<p>The Internet should not normally be used for private or leisure purposes; it is provided primarily for education or business use.</p> <p>Staff may use the internet for other purposes provided that:</p> <ul style="list-style-type: none"> • Such use is occasional and reasonable; • Such use does not interfere in any way with your duties and • You follow the code of practice at all times. <p>The Trust will not be liable under any circumstances for any injury, distress, loss or damage to staff, pupils or parents, which may arise directly or indirectly from the use of Internet facilities, the use of email or from other person's unauthorised use of those facilities or email.</p>
<p>Inappropriate material</p>	<p>Staff must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be considered to be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. "Inappropriate" in this context includes material which is unsuitable for viewing by children. Staff are responsible for rejecting any links to such material which may appear inadvertently during research.</p> <p>If staff encounter any material which could be regarded as offensive, they must leave that website or service immediately and not make any copy of that material. If staff encounter any difficulty in leaving a website or service you must inform the ICT support staff immediately.</p>



<p>Web blogs and web publishing.</p>	<p>The rules detailed in Section 3 below are also applicable to web logs or blogs and web publishing.</p> <p>Using images of children for publicity purposes requires the age appropriate consent of the individual concerned and their legal guardians. Images should not be published on websites or in publications without the appropriate consent.</p>
<p>Misuse, abuse and access restrictions</p>	<p>Staff must not misuse or abuse any website or service, or attempt to bypass any access controls or restrictions on any website or service.</p> <p>Access to some websites is blocked by Castleford Academy Trust. If staff have a genuine reason to access a blocked website please see a member of the IT Support Team.</p> <p>No unauthorised contract, purchase or payment should be made over the Internet.</p> <p>Use for personal financial gain, gambling, political purposes or advertising is forbidden.</p> <p>Consent must be in place from pupils and parents before any personal data i.e. names and photographs are published on website. Pupil’s names should never be published in full.</p>
<p>Monitoring</p>	<p>The internet access system used by the Trust maintains a record which identifies who uses the facilities and how they are used by individuals. The information collected includes which website and services staff visit, how long staff remain there and which material staff view. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings.</p>
<p>Giving out information</p>	<p>Staff must not give any information concerning the Trust, its pupils or parents or any member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people, the only exception being the use of the names when accessing a service through an agreed subscription.</p>
<p>Personal safety</p>	<p>Staff should take care with whom they correspond. Staff should not disclose their location, nor arrange meetings with strangers, they have contacted over the internet.</p>
<p>Hardware and software</p>	<p>Staff must not make any changes to any of the Trust’s hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by the Trust are an important part of the Trust’s security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage systems.</p> <p>Before purchasing hardware or software checks should be made with the IT support team.</p>
<p>Copyright & Intellectual Property</p>	<p>Staff should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner’s rights. Staff must not copy, download or plagiarise material on the internet without the express permission of the owner. Intellectual property rights must be respected.</p>



Social contact with Pupils (current and former)	Internet, email and approved contact details should be the only means used by members of staff to contact pupils, children or young people. Staff should not give their personal details such as home or phone number, Instant Messenger identities, personal email address or any other unapproved method to pupils.
Cyberbullying	<p>All forms of bullying, including cyberbullying, are taken very seriously. Bullying is never tolerated and it is not acceptable for any user to behave in a manner which is intimidating, threatening or in any way discriminatory.</p> <p>If an allegation is received that a user is responsible for comments made on line which could be deemed harmful, threatening, defamatory abusive or harassing in any way towards another employee, the academy will investigate this matter,</p> <p>Staff should not retaliate to any such incident and should report it as soon as possible to senior management.</p>

7. Section Three – E-mail policy and code of practice

The Trust’s computer system enables members of the Trust to communicate by e-mail with any individual or organisation with e-mail facilities throughout the world.

For the reason outlined above, it is essential that a written policy and code of practice exists, which sets out the rules and principles for use of e-mail by all.

Any breach of this policy and code of practice will be treated seriously and it may result in disciplinary or legal action or expulsion. The Trust may take steps, including legal action where appropriate, to recover from an individual any expense or liabilities the Trust incurs as a result of the breach of this policy and code of practice by staff.

Code of practice

Purpose	Staff should only use the Trust’s e-mail system for Trust related emails. Staff are permitted only to send a reasonable number of e-mails.
Trust's disclaimer	The Trust’s e-mail disclaimer is automatically attached to all outgoing e-mails and staff must not cancel or delete this disclaimer.
Monitoring	<p>Copies of all incoming and outgoing e-mails, together with details of their duration and destinations are stored centrally (in electronic form). The frequency and content of incoming and outgoing external e-mails are checked from time to time to determine whether the e-mail system is being used in accordance with this policy.</p> <p>The Headteachers, senior staff and technical staff are entitled to have read-only access to your e-mails.</p>



<p>Security</p>	<p>As with anything else sent over the internet, e-mail is not completely secure. There is no proof of receipt, e-mails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents.</p> <p>As with other methods of written communication, staff have to make a judgment about the potential damage if the communication is lost or intercepted. Staff must never send bank account information, including passwords, by e-mail.</p> <p>Care should be taken with the storage of confidential information. Confidential information should never be distributed through personal email.</p> <p>Members of staff found to be compromising confidentiality by use of personal email may be subject to disciplinary action.</p>
<p>Program files and non-business documents</p>	<p>Staff must not introduce program files or non-business documents from outside onto the Trust's network. This might happen by opening an e-mail attachment or by downloading a file from a web site. Although virus detection software is installed, it can never be guaranteed 100% successful, so introducing nonessential software is an unacceptable risk. If staff have any reason for suspecting that a virus may have entered the system, they must contact the ICT support staff immediately.</p>
<p>Quality</p>	<p>E-mails constitute data records and are subject to the same rules, care and checks as other written communications. All emails are confidential to the sender and recipient, unless permission has been given to read them.</p> <p>Staff should always consider whether it is appropriate for material to be sent to third parties as:</p> <ul style="list-style-type: none"> • they may have to be disclosed in legal proceedings; • they may have to be disclosed to a person if they make a request to see information held about them under data protection law; • transmitting the works of others, without their permission, may infringe copyright; <p>Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libellous, malicious, threatening or contravening discrimination legislation or detrimental to the Trust is a disciplinary offence and may also be a legal offence. This also includes postings on discussion boards and forums.</p> <p>Printed copies of e-mails need to be retained in the same way as other correspondence, in line with UK GDPR.</p>
<p>Inappropriate e-mails or attachments</p>	<p>Staff must not use e-mail to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work.</p> <p>Staff must not send personal or inappropriate information by e-mail about themselves, other members of staff, pupils or other members of the Trust community.</p> <p>Staff must never:</p> <ul style="list-style-type: none"> • open an email and / or attachment from an unsolicited source. • open an attachment from an unsolicited source or a trusted source if it seems in any way suspicious or non-work related.



	If staff receive any inappropriate e-mails or attachments, they must report these to IT support staff.
Viruses	If staff suspect that an e-mail has a virus attached to it, you must inform the IT support staff immediately.
Spam	Staff must not send spam (sending the same message to multiple e-mail addresses) without the permission of senior staff.
Storage	Old e-mails may be deleted from the server after 12 months. Staff are advised to regularly delete material they no longer require and to archive material that they wish to keep.
Message size	Staff are limited to sending messages with attachments which are up to 30Mb in size. If staff need to distribute files within an academy, they can do so by using shared areas.
Confidential Emails	Staff must ensure that confidential emails are suitably protected at all times. If working at home or remotely, staff should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential information should be encrypted or password protected before sending and deleted when no longer required.
Social contact with Pupils (current and former)	The provisions outlined above in Section two also apply to email contact. Contact through personal email addresses is not permitted and personal email addresses must not be issued to pupils.

7.1. E-mail Policy – advice to staff

Staff should remind themselves of the sections of this policy which relates to the monitoring, security and quality of e-mails. In addition, staff should be guided by the following good practice:

- Staff should check their e-mails on a daily basis and respond, as appropriate, within a reasonable period, usually within 48 hours for email addressed directly to staff;
- Staff are not expected to respond to emails outside of work hours;
- Staff should avoid using the e-mail system as a message board and thus avoid sending trivial global messages. Whilst accepting the convenience of the whole staff and teaching staff distribution lists staff should try to restrict its use to important or urgent matters;
- When global distribution is used, staff should be as specific as possible in the title to so as to alert staff of the content and relevance of the e-mail;
- Staff should send e-mails to the minimum number of recipients;
- Staff are advised to create their own distribution lists, as convenient and appropriate;
- Staff should always include a Subject line;
- Staff are advised to keep old e-mails for the minimum time necessary.



Further Guidelines

- Remember that e-mails remain a written record and can be forwarded to others or printed for formal use;
- As a rule of thumb, only write what they would say face to face, and should avoid the temptation to respond to an incident or message by e-mail in an uncharacteristic and potentially aggressive fashion. Remember “tone” can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression;
- Remember that sending emails from their account is similar to sending a letter on academy/trust letterhead, staff should not write anything that might bring discredit or embarrassment to themselves, the Trust, its business, employee, suppliers or anybody linked to Castleford Academy Trust;
- Not create or send communications which are defamatory or derogatory;
- Never send sensitive or confidential information – unless appropriate password protection is applied;
- Not create communications which are intimidating, hostile or offensive in any way;
- Be aware that copyright law also applies to all communications.

8. Section Four – Social media use and code of practice

Code of practice

1.	Staff should set their profiles to private and ensure they do not accept friend requests from pupils or parents.
2.	Members of staff must not have contact with any pupils, through sites and staff must not add pupils, children or young people or parents as ‘friends’ or respond to friend requests from children if asked on social media sites. If a member of staff suspects than an existing friend is a former or current pupil, they should report this matter to a member of the SLT immediately (refer to the Code of Conduct for further guidance).
3.	It is recognised that personal access to Social Networking sites outside the work environment is at the discretion of the individual however, 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.
4.	Secure and suitable strength passwords should be devised and security settings should be applied so access to profiles and the information contained is limited to those explicitly given access.
5.	Personal profiles on social networking sites and other internet posting forums must not identify the Trust as a 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 post by staff is considered inappropriate or could be considered to bring the Trust or profession into disrepute, disciplinary action may be considered.



9. Appendix 1 – Live Lessons – Staff Protocol

In the event of an academy closure, the following procedure will apply for the delivery of live lessons.

- Staff must always observe professional conduct.
- Staff must continue to follow the academy's safeguarding procedures and policies during all live lessons. If they are concerned about a child, they need to report this to the safeguarding team as soon as possible.
- If staff are delivering at home, this should be in a suitable room without distractions from colleagues, family member, pet, etc.
- Pupils should not be able to hear personal conversations.
- Staff should work with an appropriate background for live lessons (avoid fake backgrounds as this can be distracting). Personal information about staff, family members or other pupils should not be visible to pupils.
- Staff are representing the Trust so should be dressed appropriately.
- A live lesson will be treated the same as a classroom lesson. Behaviour expectations of pupils will apply. If the behaviour of a pupil does not meet staff expectations, staff can remove them from the live lesson.
- During the lesson, staff should not engage in communication with parents.
- All pupils have been asked to place their devices on mute. If they wish to speak to their teacher, they must do so using the raise hand icon.
- Pupils will not have access to a mobile phone during the lesson unless they are accessing the lesson through a mobile phone. If this is the case, they must not engage with social media or messaging systems during the lesson.