Chorus Education Trust

ICT Acceptable Use Policy

Important: this document can only be considered valid when viewed on the Trust or School website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

Version number:	1.3
Implementation date:	December 2019
Next review:	September 2021
Name and job title of author:	Richard Clough, IT Director
Target audience:	Students / Staff / Trainees / Parents / Governors / Trustees / Visitors
Related documents:	Staff Handbook Staff Communications Policy

Chorus
Education Trust

Contents

Policy Statement

The purpose of this policy is to ensure that employees, workers, students and other people accessing Chorus Trust Information Communication Technology (ICT) understand the ways in which the ICT equipment is to be used. Our aim is to provide a service within schools to promote educational excellence in ICT, innovation, communication and educating users about online behaviour. This includes interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness. The policy aims to ensure that ICT facilities and the Internet are used effectively for their intended purpose, without infringing legal requirements or creating unnecessary risk. Where reference is made to Trust ICT, this also includes any school specific facilities, equipment and networks. Any reference to Trust includes its schools.

Employees are provided with free access to a wide range of ICT provision to enable and assist their work and support their educational development. By using the Trust's provision all users are agreeing to this 'Acceptable Use Policy'. When logging on to any computer in the Trust, users are presented with an informational message that alerts them to the fact that they are bound by the terms in this, and all related policies. All users must click 'OK' to show that they agree to the policies before they can continue to use the systems. This action is considered as further agreement to the terms of these policies.

Users are responsible and personally accountable for their use and activity on the Trust's ICT systems. Any use that contravenes this policy may result in the Trust Disciplinary Policy and Procedure being invoked. In addition, ICT usage privileges may be withdrawn or reduced.

1. Scope

This policy applies to all employees, workers, students and others accessing ICT at Chorus Education Trust and they will be termed as 'users' within this policy. This policy details the Trust's expectations of all users of the Trust's electronic communication, including, but not limited to telephone, email, internet and ICT systems.

2. Roles and Responsibilities

The Trust Board is responsible for monitoring the effectiveness of this policy, ensuring that a consistent approach to ICT is applied across the Trust.

The CEO is responsible for ensuring that staff and managers are aware of and adhere to this policy and procedure and that breaches are managed swiftly and effectively.

The IT Support Team is responsible for ensuring that all employees understand their responsibilities when using ICT at work and that systems are used and managed effectively. The IT Support Team will limit access to websites and may be directed to monitor usage and report any breaches to the Head of School, Executive Principal or CEO.

Managers must ensure they report any breaches of this policy immediately to the IT Support Team or Head of School.

All users must ensure they understand and adhere to the Trust's expectations regarding electronic communications, seeking further clarification and advice where appropriate.

3. Key Principles

This policy details the minimum expectations of the Trust when users are accessing Trust communication systems. Failure to comply with these requirements may be viewed as an abuse or misuse of the systems and a breach of this policy could be viewed as a disciplinary matter, with serious breaches potentially leading to dismissal. Users are encouraged to use remote access rather than memory sticks in line with General Data Protection Regulations (GDPR).

- Passwords and login details must remain confidential.
- Users must not intentionally install software unless specifically authorised to do so.
- Users must not intentionally introduce viruses or other malicious software.
- Act in a way that contravenes the Code of Conduct, other policies, legislative, statutory or professional requirements.
- Bring the Trust/School into disrepute.
- Disclose sensitive information or personal data to unapproved people or organisations.
- Breach the General Data Protection Regulations.
- Intentionally access or download material containing sexual, discriminatory, offensive or illegal material.

- Participate in online gambling, including lotteries.
- Participate in online auctions unless authorised to do so for work-related matters.
- Originate or participate in email chain letters or similar types of communication.
- Participate in chat rooms/forums unless this is work-related or for professional purposes.
- Harass or bully any other person.
- Create material with the intent to defraud.

The Trust's communications systems must not be used to:

- Store, send or distribute messages or material which may be perceived by the recipient or the Trust as:
  - Aggressive, threatening, abusive or obscene.
  - Sexually suggestive.
  - Defamatory.
  - Sexually explicit.
  - Discriminatory comments, remarks or jokes.
  - Offensive.

If a user accidentally accesses inappropriate material on the internet or by email, they must immediately close down the email/programme and inform their manager or IT Support. Users are encouraged to only use white boards/projectors where appropriate (e.g. for publicly sharing information as opposed to checking emails). Users are also advised not to facilitate students or other adults (e.g. third-party providers) bringing inappropriate material into school (e.g. films that are rated for adults rather than children). Wherever possible, users working with third parties should review the materials the third-party providers wish to use to ensure they are appropriate in relation to the audience and the school and Trust policies and procedures.

Users must not bring into school any material that would be considered inappropriate on paper. This includes files stored on memory sticks, CD, DVD or any other electronic storage medium. Under no circumstances should any users of the Trust or school's ICT systems download, upload or bring into school material that is unsuitable for children or schools. This includes any material of a violent, racist or inappropriate sexual nature. The transmission, display, storage or promotion of any such material is a violation of the Computer Misuse Act 1990, and possession of certain types of material can lead to police prosecution. If in any doubt, staff should check with their line manager or the IT Department. Staff are also encouraged to refer to the film classification system as a guide.

Users must not use the Trust or school's ICT systems for the creation or transmission of content that promotes extremist activity, including terrorism and weapons and users must not post any information on websites or social media that could cause any other member of the Trust or schools distress, or bring the Trust or its schools into disrepute.

Occasional appropriate and reasonable personal use of e-mail and the Internet, and IT equipment, is permitted provided such use of the Trust or school systems:

- Is restricted to the user's own time.
- It doesn't interfere with the performance of duties.

- It doesn't adversely impact on the performance of the Trust or a school's communication systems or the network.
- It doesn't involve storing private information or information/data not connected to normal duties.
- It isn't for the purpose of furthering outside business interests.
- It doesn't contravene the requirements of the Trust's Code of Conduct, other Trust or school policies.

Users must always be mindful that they are responsible and personally accountable for their use and activity on the Trust and school's ICT systems. Misuse of the communication systems belonging to, or associated with the Trust or any of its schools may breach the Code of Conduct, other policies and/or procedures and/or the law. Users can be held personally liable and such breaches may lead to civil, criminal or disciplinary action including dismissal.

Users are responsible for all files that are stored in their storage area and any visits to websites via their user account. Users may not use any of the Trust's ICT systems for private financial gain, or any political or commercial activity, other than for official trade union activities. Users must not breach the copyright of any materials whilst using the Trust's ICT systems. This includes, but is not exclusive to:

- Copying, or attempting to copy, any of the school's software.
- Storing any files in their personal storage area which require copyright permission, and where that permission is not held.

Any breach of copyright whilst using the Trust's ICT systems is the individual user's responsibility and the Trust cannot accept any liability or litigation for such a breach.

Users must ensure that:

- They keep personal data safe, taking steps to minimise the risk of loss or misuse of data.
- Personal and sensitive, confidential data is protected with the use of passwords, locking of computers, logging off shared devices, use of encryptions where appropriate and increasing the use of remote access rather than transporting or transferring information.
- Personal, sensitive and confidential data must not be stored on any form of removable media (e.g. memory sticks, external hard-drives, CDs or DVDs) and it must not be stored on users' personal devices (e.g. home PCs, mobile 'phones).
- When using mobile devices (e.g. surfaces and laptops) users encrypt/password protect documents; password protect the device; ensure the device has appropriate virus and malware checking software.
- Data is only retained, destroyed and deleted safely in line with the Trust's Data Protection Policy and associated procedures and guidelines.

Users must not download, copy or attempt to install any software onto Trust computers without checking first with their line manager and the IT Department. Any attempt by a user to compromise the security or functionality of the Trust networks and its ICT systems, from either internally or externally, will be considered as "hacking". It should be noted that "hacking" is illegal under the Computer Misuse Act 1990 and is prosecutable under law. Users must not deliberately attempt to gain unauthorised access to networked facilities or services, including any attempt to probe, scan or test the vulnerability of the system

or network. All machines connected to the Trust's ICT networks, must have appropriate, fully functioning and up to date antivirus software protection. If unsure, staff should seek advice from the IT Department.

Users must not discuss or post content that reflects the Trust or its employees in an inappropriate or defamatory manner through any electronic communication methods. This includes posting to social networking sites.

Users must not carry out any of the following deliberate activities:

- Corrupting or destroying other users' data.
- Violating the privacy of other users.
- Disrupting the work of others.
- Denying service to other users (for example, by deliberate or reckless overloading the network).
- Continuing to use an item of networking software or hardware after the Trust or school has requested that use cease because it is causing disruption to the correct functioning of the school's ICT systems.
- Other misuse of the Trust and school's ICT and networked resources, such as the introduction of viruses or other harmful software to the school's ICT systems.
- Unauthorised monitoring of data or traffic on the Trust or school's ICT network or systems without the express authorisation of the owner of the school's network or systems.

This policy still applies when users access any of the Trust's systems from home or an external location.

When accessing another network from the Trust's ICT networks, any breach of this policy will be regarded as unacceptable use of the Trust's ICT systems.

The Trust wishes to encourage all users to use the internet, however it is provided for work purposes and any use of the internet for personal reasons must be carried out in the user's free time. The Trust cannot be held responsible for any failed personal financial transaction that may happen whilst using the Trust's ICT systems.

Any attempt to circumvent the Trust's firewall and internet filtering systems will be treated as a breach of this policy. This includes the use of proxy servers and websites to bypass the internet filtering systems. Such activity will be subject to the Trust's Disciplinary Procedure and in addition to any disciplinary outcome or sanction, it could also result in the removal of access to the Trust's ICT systems or internet access.

There is a wealth of information on the internet; however due the open nature of the internet, some material is either illegal or unacceptable. Any user that thinks inappropriate or illegal material is being accessed must report it to their line manager or the IT Support Team. Any user found intentionally accessing such material will be subject to the Trust's Disciplinary Procedure.

Users should:

- Limit personal use of the internet to reasonable levels and own time.
- Represent themselves honestly and accurately when using the internet to participate in social networking.
- If users accidentally access inappropriate material including unexpected 'pop-ups' they must disconnect immediately and inform their line manager and/or the IT Support Team.

Users must not:

- Access or download material, which is offensive, sexually explicit, discriminatory or illegal.
- Use systems to participate in on-line gambling or on-line auctions.
- Download music or video files unless for Trust or school purposes.
- Use 'peer to peer' or other file sharing services except where authorised to do so.

4. Email and Electronic Acceptable Use

The Trust expects all users of Trust electronic devices/servers/Wi-Fi to use email and electronic communication responsibly and strictly according to the following conditions.

- Email facilities are provided as a method of enhancing communication of work and school related issues. All users are responsible for the content of the messages that they send.
- All email communication can be intercepted at any point between the user and the recipient. The safest thing is to assume that sending an email is the same as sending a letter.
- Users are reminded that electronic communication can be monitored, and random checks may be made.
- When sending an email, the same care and consideration should be taken as when sending a letter on Trust letter headed paper as users are communicating on behalf of the Trust.
- Email is the equivalent of a written document and can be used as an evidential record. With this in mind care and consideration should always be taken before sending an email (e.g. freedom of information requests and subject access requests).
- Where there is a concern that a user has misused the email system, action may be taken in line with the Trust's Disciplinary Procedure.
- All electronic communication between staff and students must be carried out through the Trust's ICT systems.
- The Trust does not expect employees to respond to work emails outside of normal working hours.

Staff should not communicate with students via social network sites, texts or telephone calls. Staff must not divulge personal contact details (mobile telephone numbers, non-work email addresses, social networking sites etc.) to students and any unintended breach must be reported to the IT Support Team and the user's line manager immediately.

Users who receive emails regarding viruses or security threats must delete the email and report to the IT Support Team. Users can minimise the risk of inadvertently introducing viruses by permanently deleting without opening emails that look suspicious. Staff are encouraged to contact the IT Support Team for advice and concerns that a virus may have entered a Trust system should be reported to the IT Support Team immediately.

Users should:

- Limit personal use of email and texts and personal email and texts should only take place in their own time.
- Ensure that their messages are relevant and appropriate to targeted recipients (e.g. not using 'blanket' or 'all-user' emails).
- Delete messages that are no longer needed.
- Try to answer emails quickly, politely and professionally.
- Beware of 'email rage'. Email is quick and easy to use and can encourage ill-considered and even offensive messages.
- Include a subject heading in every email so that the person receiving it knows what it is about.
- Type emails carefully, making sure that grammar and spelling are correct - an email is just like a letter and users can expect it to have the same effect.
- Remember that emails have the same legal status as letters and need wording with care (e.g. they must be released if requested via Freedom of Information Requests).
- Use plain text email messages -this means smaller electronic message sizes and reduces some virus risks.
- Inform management immediately if the user receives or sees any offensive or sexually explicit material on the intranet or in email messages at work.

Users must not:

- Use their own devices, including mobile phones, in classrooms in front of students.
- Use a password in a way that can be seen by students.
- Use email to circulate material, which is offensive, illegal, discriminatory, extremist or sexually explicit.
- Use email as a substitute for good verbal communication.
- Send personal information or confidential or sensitive material using external email – it may be accessed unlawfully. This may include bulk forwarding of emails to your own external account.
- Originate or participate in email chain letters or messages.
- Use the Trust or school email systems to distribute material of a political nature.
- Expect to receive a response to emails outside of normal working hours.

If staff are in doubt they should seek advice from their line manager or the IT Support Team.

5. Social Media and Acceptable Use

Social networking websites provide an opportunity for people to communicate 'en masse' and share ideas regardless of geographic distance. Sites such as Facebook, Twitter and LinkedIn can serve as a learning tool where training videos and other materials are made easily accessible to students in a user-friendly and engaging way. They can also be a useful tool for schools to communicate key messages to their community and the wider public. However, the open nature of the internet means that social networking sites can

leave professionals vulnerable if they fail to observe a few simple precautions. The below guidelines are intended not as a set of instructions, but general advice on how to avoid compromising your professional position. Staff should also consult the ***Staff Communications Policy*** for further advice.

Privacy

Staff should ensure their Facebook accounts do not compromise their professional position and they should ensure that their privacy settings are set correctly. The Trust expects staff to take reasonable steps to ensure their social media presence is private with appropriate restrictions in place and where there is the potential for a breach, staff are expected to declare to their line manager what they reasonably know. Staff should also be aware that settings can change, and they should also regularly review their list of friends.

Staff must not under any circumstances knowingly accept friend requests from a person they believe to be either a parent or a student at a school within the Trust. The exception to this is if an employee's own child(ren) attend a Trust school or if close friends have children at a Trust school or are employed by the Trust. In these circumstances, it is accepted that communication can take place and that images of their own children and their friends when at parties or such similar personal events may be posted. Care should be taken to ensure the suitability of the images and to use appropriate security settings. Images must not be posted in relation to the school. Staff should seek advice from their line manager in such circumstances.

As a minimum, the Trust recommends the following:

Privacy Setting Recommended Security Level – Facebook

Facebook is a published and open social media site and information is therefore available to the public.

- Send the user messages - friends only.
- See the user's friend list - friends only.
- See the user's education and work - friends only.
- See the user's current city and hometown - friends only.
- See the user's likes, activities and other connections - friends only.
- View the user's status, photos, and posts - friends only.
- Family and relationships - friends only.
- Photos and videos - friends only.
- Religious and political views - friends only.
- Birthday - friends only.
- Permission to comment on your posts - friends only.
- Places you check in to - friends only.
- Contact information - friends only.

Users must always make sure they log out of Facebook after using it, particularly when using a machine that is shared with other colleagues/students. The user's account can be hijacked by others if the user remains logged in – even if they quit the browser and/or switch the machine off. Similarly, Facebook's instant chat facility means conversations can be viewed later on. Users must ensure they clear their chat history on Facebook (click "Clear Chat history" in the chat window).

Conduct on social networking sites

- Users should not make disparaging remarks about their employer/colleagues.
- Users must act in accordance with this policy and any specific guidance on the use of social networking sites.
- Users are encouraged to think about any photos they may appear in and on Facebook they may wish to 'untag' themselves from a photo.
- If a user finds inappropriate references to themselves and/or images of them posted by a 'friend' online, they are encouraged to contact them and the site to have the material removed.
- Staff are reminded that parents and students may access their profile and could, if they find the information and/or images it contains offensive, complain to the Trust.

If users have any concerns about information on their social networking sites or if they are the victim of cyber-bullying, they should contact their line manager.

If users believe someone has established a fake account using their details, they must inform their line manager and the IT team at their earliest opportunity.

When using social media users must not:

- Make defamatory statements about the Trust, its schools or its employees.
- Post messages that are unlawful, libellous, harassing, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented or racially offensive.
- Post content copied from elsewhere, for which the user does not own the copyright.

Under no circumstances should a member of staff have students as friends on social networking sites without seeking prior permission from their line manager and where it is necessary and appropriate for the member of staff to have students as friends (e.g. family members) they must complete the declaration form (appendix 1).

6. Monitoring

Authorised officers or staff of the Trust and its school's ICT providers may at any time monitor the use of Trust and school communications systems. The use of all Trust communications systems particularly email and the internet is subject to recording in order to detect and deal with abuse of the systems and fault detection, including access to Trust servers and Wi-Fi. Neither the Trust nor any of its schools will, without reasonable cause, examine any private material that is discovered.

Personal data should not be stored on the network and users should not expect 'privacy' in relation to accessing websites, personal email correspondence, personal documents stored on Trust ICT equipment or networks or messages sent via the internet, as these, in principle, are subject to the same checking procedures applied to business related access and email correspondence.

7. Passwords

The Trust is responsible for ensuring data and the network is as safe and secure as possible. A weak password may result in the compromise or loss of data. As such, all users are responsible for taking the appropriate steps, as outlined below, to create and secure their passwords.

The aim of passwords is to protect user's data, children's welfare where access to confidential and sensitive data is allowed and to also minimise the risk of unauthorised access to the Trust and school networks.

- Passwords should be changed every 90 days
- Passwords will be a minimum of 8 characters
- Passwords should not contain the user's account name or parts of the user's full name that exceed two consecutive characters. They should contain characters from three of the following four categories:
    - Uppercase characters (A to Z)
    - Lowercase characters (a to z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

8. Monitoring compliance with and effectiveness of the policy

Effectiveness and compliance of this Policy will be monitored on an annual basis.

9. Review

This Policy and Procedure will be reviewed on an annual basis by the Trust with recognised trade unions at local secretary level.

Appendix 1

Declaration of Social Media Student/Parent Contact

Introduction

- All employees have a duty to declare any circumstances where they have students or parents as contacts via social media.
- The declaration enables the employee and the Trust to assess and appropriately manage any associated risks.

Question Areas

How do you know the individual(s)?
Why is social media contact with them necessary and appropriate?
What are the risks associated with this social media connection?
How can we manage and minimise these risks?
Any additional comments:

Signed by the employee:

Print name:

Signed by the line manager:

Print name:

Date: