thrive
co-operative learning trust

IT Acceptable Use Policy & Agreement

Policy reviewed and adopted by the Board of Trustees:	March 2021
Version:	2
Date of next review:	Spring 2022
Responsible Committee:	Finance and Personnel
Monitoring:	Trust Board

Contents

Introduction

Our vision, underpinned by co-operative values[1], is threefold; to work in partnership with the community we serve to combat social exclusion and deprivation, to build a sustainable and vibrant community and local economy, and to provide learners with a global perspective helping them to become responsible and articulate citizens in a global economy. We will achieve this by delivering the highest possible standards of education, and for this we rely on the appropriate conduct of all our employees and volunteers.

Thrive welcomes the support of recognised Trade Unions in seeking to implement this policy in a fair and consistent manner.

Purpose

The main purpose of the policy is to ensure that staff and volunteers understand how the Trust requires them to act responsibly and appropriately when using digital technology at school, on Trust devices out of school, and on digital platforms managed by Thrive (e.g. Thrive domain Google products).

The acceptable user policy recognises the increasing importance of the use of new and evolving technologies within the lives of all and in particular within the business and administration uses of the Yorkshire and the Humber Co-operative Learning Trust. In today's environment access and use of efficient systems is a must. All users should therefore have an entitlement to safe access to the internet and digital technologies at all times.

The frequently asked questions element of this document is part of the policy.

This Acceptable Use Policy is intended to ensure;

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that the Thrive Co-operative Learning Trust (Thrive) systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

Thrive will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of all IT systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, as appropriate, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

[1] self-help, self-responsibility, democracy, equality, equity, solidarity, honesty, openness, social responsibility and caring for others

For my professional and personal safety:

- I understand that Thrive will fulfil its obligations and legal safeguarding duties (including 'Prevent) by reviewing any reported use of internet search phrases logged by internal software and will bring these to my attention as appropriate (details on how we will do this are given in appendix 1).
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE, Google products etc.) in any environment on or off a Thrive physical site. This also applies to the use of any personal data (digital or paper based) to which I have access.
- I understand that ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by Thrive.
- I will not share a Trust device within my household or family.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person, usually Designated Safeguarding Lead.
- I will close any webpages used for personal use on my device before connecting it to school WiFi.

I will be professional in my communications and actions when using IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I will respect the opinions of others where they differ from my own.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the relevant policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school/Trust websites / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in accordance with the relevant policies.
- I will only communicate with students / pupils and parents / carers using official IT systems, such as my Thrive Google Mail account. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

Thrive have the responsibility to provide safe and secure access to technologies and ensure the smooth running of each academy/schools' IT systems:

- When I use my personal mobile devices (laptops / tablets / mobile phones / USB devices etc) for work related business, I will follow the rules set out in this agreement, in the same way as if I were using Trust owned equipment. I will also follow any additional rules set by the Trust about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- Removable devices such as USB external hard drives and USB memory sticks must be encrypted before being used to store Thrive data. Please speak to IT Services who will be able to encrypt your device for you. Non-encrypted drives are not permitted.
- Trust owned Mobile Phones must be secured by a pin code/password or fingerprint.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my work is regularly backed up, in accordance with relevant Trust policies. This includes data stored on personal/school/Trust owned removable drives.
- I will not try to upload, download or access any materials which are illegal (including child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes on a Trust owned device , or store programmes on a computer, nor will I try to alter computer settings, unless this is authorised by IT Services.
- I will not disable or cause any damage to Trust equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable secure storage. All losses of such data must be reported immediately to my School Business Manager who will liaise with the Trust Data Protection Officer.
- I understand that the Data Protection Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by a Trust policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- The loss or theft of removal storage devices, containing Trust data and Trust owned laptops must be reported to IT Services immediately.

When using the internet in my professional capacity or for Trust sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- When I access the internet for personal use this will not compromise my duties and will not be during agreed working hours.

I understand that I am responsible for my actions in and out of my normal place of work:

- I understand that this Acceptable Use Policy applies not only to my work and use of Trust digital technology equipment, but also to my use of IT systems and equipment off site and the use of any personal equipment for Trust purposes.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action or any other action pertinent to my role. This could include a warning, a suspension, and in the event of illegal activities the involvement of the police. Any such activity may constitute gross misconduct which could lead to dismissal.

I have read and understand the above and agree to use IT digital technology systems (both in and out of my normal place of work/activity) and my own devices (within the Trust and when carrying out communications related to the Trust) within these guidelines.

Consent

The Trust will gain your consent sent via a Google Form sent to your email address. School Business Managers will be tasked with ensuring that all staff have given consent. Failure to consent may become a disciplinary matter.__

Appendix 1 - Frequently Asked Questions

Can the Trust see what I am looking at on the internet?

The Smoothwall web filtering system at each school will log all internet activity for all users. This is only whilst your laptop, PC or a mobile device which is connected to school WiFi is being used. This is not the case when using your device at home. The only exception to this is when you are using the remote access service which is the same as using a computer in school.

The Smoothwall will also log any attempt to access websites or perform a web search for terms which are listed under the PREVENT categories such as radicalisation, terrorism, as well as pornography. A report of such attempts are automatically reported to the school's Designated Safeguarding Lead each day for review.

For secondary school computers that stay in school, the Securus Safeguarding monitoring software will also 'screenshot' any content accessed or created which is categorised as a PREVENT term.

Can I use a Trust device to browse the internet in the evening or at a weekend?

Yes, you are welcome to use a Trust loaned device in the evening as long as it is used in accordance with this Acceptable Use Policy. It is important that you close down personal information and exit websites viewed before reconnecting to school WiFi.

Can family members or friends use my Trust loaned computer?

No, the laptop which you have been loaned by the Trust is for your use only. You are responsible for the device at all times until it is returned.

If I connect my personal mobile phone or tablet to the school's WiFi, will this be monitored?

Yes, all devices connected to WiFi will be monitored by the school's Smoothwall web filtering system as described above. Any open browser material will be picked up by the school's Smoothwall as the device connects to the school WiFi.

Lesson planning may require me to search for words like 'abuse', 'radicalisation' or 'female genital mutilation'. Would this be logged?

Yes, the Smoothwall would log the attempt to access such sites under the PREVENT categories of keywords. These would be automatically reported to the school's Designated Safeguarding Lead who will approach you sensitively and professionally to discuss as appropriate.

Can documents that I create or emails that I send be seen by the Trust?

Google has a facility called Google Vault which allows IT to search for and recover deleted documents or emails. IT would be able to search for documents or emails using keywords in the Google Vault system for all or individual users. Please note that a request for a search will be passed to the Chief Financial Officer for approval.

Can I use my personal mobile phone, tablet or laptop to access Email or the school's remote access system?

Yes, but please ensure you log out of such systems when you are finished and protect your mobile phone with a PIN code/face ID if available.