THE EDUCATION ALLIANCE

ICT Acceptable Use Policy

Version 4.2

Important: This document can only be considered valid when viewed on TEAL's 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. **Name and Title of Author:**	Lisa Longstaff, Director of People and Matt Wadsworth, Director of IT
Name of Responsible Committee/Individual:	Executive Board
Implementation Date:	Summer Term 2024
Review Date:	Summer Term 2026
Target Audience:	All users of TEAL ICT (hardware, software and wi-fi)
Related Documents: All Trust policies and procedures referred to are located on the trust website, www.theeducationalliance.org.uk. If English is not your first language, and you require assistance/translation, please contact the HR Department. This policy has been equality impact assessed.	Expectations and Code of Conduct Data Protection Policy Whistleblowing Policy Grievance Procedure Use of Equipment and Assets Policy Child Protection and Safeguarding Policies Disciplinary Policy and Procedure Teachers' Standards Mobile Phone Policy

Contents

Appendices

POLICY STATEMENT

We are here to make great schools and happier, stronger communities so that people have better lives. We do this by:

- Always doing what is right
- Trusting in each other and standing shoulder to shoulder
- Doing what we know makes the difference

Doing what is right means always acting with integrity, in the interests of others and being honest, open, and transparent.

Employees are provided with free access to a wide range of information communication technology (ICT) provision to enable and assist their work and support their learning and development. We aim to ensure users of the Education Alliance (TEAL/the trust) ICT use it safely, operating within legal and statutory frameworks, expectations, our culture, and ethos.

1. SCOPE

This policy applies to all employees, workers and others accessing ICT at TEAL and they will be termed as ‘users’ within this policy, and it details TEAL’s expectations of all users of TEAL’s electronic communication, including, but not limited to telephone, social media platforms, email, internet, and ICT systems.

The purpose of this policy is to ensure that users understand the ways in which the ICT equipment, software and wi-fi is to be used. 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 TEAL ICT, this also includes any school specific facilities, equipment, and networks. Any reference to TEAL includes its schools, central services, and Yorkshire Wolds Teacher Training (YWTT). This policy still applies when users access any of TEAL's systems off-site.

By using TEAL's provision, or using personal devices onsite, all users are agreeing to adhere to this policy. When logging on to any TEAL computer, 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, including monitoring information.

2. ROLES AND RESPONSIBILITIES

The **Executive Board** is responsible for approving this policy.

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, effectively, fairly, and consistently.

The **IT Helpdesk** 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 Helpdesk will limit access to websites and may be directed to monitor usage (e.g. where there are allegations of misconduct) and report any breaches to the Headteacher or a member of the Executive Team.

All users must ensure they report any breaches of this policy immediately to the IT Helpdesk, Headteacher or the Executive Team. Data protection breaches must also be reported to the relevant member of the Executive Team.

All **users** must ensure they understand and adhere to TEAL's expectations regarding electronic usage and communications, seeking further clarification and advice where appropriate. If they require access to a website, which is blocked, they should raise the issue with their line manager and the IT Helpdesk.

3. EQUALITY AND DIVERSITY

TEAL is committed to:

- Promoting equality and diversity in its policies, procedures, and guidelines
- Ensuring staff are protected from unlawful direct or indirect discrimination resulting from a protected characteristic (e.g. age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation).

When this policy is reviewed, equality information will be shared with the Executive Team and the Joint Consultation and Negotiation Committee, to ensure we are able to check for any unintended disadvantages linked to TEAL policy and practice.

4. KEY PRINCIPLES

Users must ensure they act responsibly in their use of ICT, keeping data safe (e.g. using passwords, sharing protected links rather than documents where possible and keeping login details confidential). Users must not intentionally install software unless specifically authorised to do so, and they must not intentionally introduce viruses or other malicious software. By following this policy and associated guidance, users can help TEAL guard itself from cyber-attacks and data breaches.

Users are asked not to identify themselves with TEAL on their personal social media accounts, and they are advised to ensure their social media profiles are 'private' so that pupils and parents do not have access to their personal details and images. Users should be aware that they leave themselves open to a charge of professional misconduct if inappropriate images of them are made available on a public profile. They are advised to exercise caution and not to accept friend requests from parents other than where close personal or familial relationships already exist.

When using ICT for work purposes, users must not:

- Act in a way that contravenes TEAL's Expectations and Code of Conduct, other TEAL, or school policies, legislative, statutory, or professional requirements
- Disclose sensitive information or personal data to unapproved people or organisations
- Breach TEAL's Data Protection Policy and associated procedures
- Intentionally access, download or share material containing sexual, discriminatory, offensive, illegal material; communicate in a way or with information that could be viewed to be aggressive, threatening, abusive, obscene, sexually suggestive/explicit, or defamatory.
- Allow current or recent pupils access to their social media accounts, including adding them as 'friends', except in cases where permission has been given by the Headteacher (e.g. alumni groups). It is the employee's responsibility to ensure that their accounts and passwords are secure, and any potential breach should be reported to the Headteacher immediately.
- Use a password in a way that can be seen by pupils
- Use email to circulate material which is illegal or does not align with TEAL expectations expect to receive a response to emails outside of normal working hours, or an immediate response, as not all staff can easily access their emails throughout the working day.

If a user accidentally accesses inappropriate material on the internet or by email, they must contact the IT Helpdesk.

Users must not bring into school any material that would be considered inappropriate. This includes files stored on memory sticks, CD, DVD, or any other electronic storage medium, or accessing information via TEAL's wi-fi, which would be viewed inappropriate. Under no circumstances should any users download, upload, or bring into school material that is unsuitable for children or schools. 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 Helpdesk.

Accessing, marketing, and storing child pornography or indecent images of children is illegal and is likely to lead to a criminal conviction and the individual being barred from working with children and young people. Under no circumstances should employees use TEAL equipment to access inappropriate images on the internet or access any other site which could call into question their suitability to work with children. The same rule applies to the use of TEAL's equipment by employees at home (e.g. laptops and tablets).

Users must not to communicate with pupils via social network sites, texts, or telephone calls. If users are unsure, they should seek advice from their line manager in the first instance. Users must not share personal contact details with pupils (mobile telephone numbers, non-work email addresses, social networking sites etc.) and any unintended breach must be reported to the IT Helpdesk and the user's line manager immediately.

If an employee becomes aware that they are in an online game with a pupil, they should cease the game immediately. Under no circumstances should employees seek out pupils or share identity tags or usernames with them to play online games.

Users are advised (e.g. through briefings and pop-up information) that internet-based activity on personal devices is monitored and logged whilst using TEAL's wi-fi, and misuse of TEAL ICT systems and networks may breach TEAL's Expectations and Code of Conduct, other policies and/or procedures and/or the law. Any attempt by a user to compromise the security or functionality of TEAL networks and its ICT systems, 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. Any attempt to circumvent TEAL'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. 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 by their user account. Users must not breach the copyright of any materials whilst using TEAL'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 TEAL's ICT systems is the individual user's responsibility and TEAL 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.
- Personally identifiable 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 linked files and cloud-based operations.
- Personally identifiable, sensitive, and confidential data must not be stored on any form of removable media (e.g. memory sticks, external hard-drives, surfaces or laptops, and 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) they encrypt/password protect documents; password protect the device; and ensure the device has appropriate virus and malware checking software.
- Data is retained, destroyed, and deleted safely in line with TEAL's Data Protection Policy and associated procedures and guidelines.

Users should ensure:

- 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)
- include a subject heading in every email so that the person receiving it knows what it is about
- inform management immediately if the user receives or sees any offensive or sexually explicit material, spam, or phishing communications on the intranet or in email messages at work
- not allow email and electronic communication to replace face to face communication

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

- corrupting or destroying other users' data
- violating the privacy of other users
- continuing to use an item of networking software or hardware after TEAL has requested that use cease because it is causing disruption to the correct functioning of TEAL's ICT systems and/or networks
- unauthorised monitoring of data or traffic on TEAL's ICT network or systems without the express authorisation of the owner of the network or systems

5. EMAIL AND ELECTRONIC COMMUNICATION ACCEPTABLE USE

When using TEAL equipment, networks, email, and electronic communication, we expect all users act 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. Users are reminded (e.g. via pop-up messages and briefings) that electronic communication can be monitored and checks may be made. 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).

All electronic communication between users and pupils must be carried out through TEAL's ICT systems, and TEAL has enforced 2-factor authentication when accessing email outside of TEAL buildings for users.

Users who receive emails that may pose a security threat must contact the IT Helpdesk at their earliest opportunity. Users are encouraged to contact the IT Helpdesk for advice and concerns that a virus may have entered a TEAL system should be reported to the IT Helpdesk immediately.

If users are in doubt, they should seek advice from their line manager or the IT Helpdesk.

6. MONITORING

The IT Helpdesk and TEAL's ICT providers may at any time monitor the use of TEAL's ICT systems and networks. The use of all Trust ICT systems and networks, particularly email and the internet, is subject to recording to reduce risks. TEAL will not, without reasonable cause, view any private material that is discovered. Users are advised that information held by TEAL/on TEAL devices can be disclosable for data protection purposes (e.g. subject access requests and freedom of information requests).

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 TEAL ICT equipment or networks, or messages sent via the internet, as these, in principle, are subject to the same checking and monitoring procedures applied to work related access and email correspondence.

7. PASSWORDS

We aim to ensure that 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 data and children's welfare, where access to confidential and sensitive data is allowed, and to minimise the risk of unauthorised access to TEAL's networks. Users should change their password each term, and passwords should:

- Have a minimum of six characters
- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
- Contain characters from three of the following four categories:
  - Uppercase characters (A through Z)
  - Lowercase characters (a through 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 regularly monitored by TEAL's Director of IT.

9. REVIEW

This policy will be reviewed within two years of the date of implementation with recognised trade unions via TEAL's JCNC.

Appendix 1

SOCIAL MEDIA GUIDANCE

Introduction

This guidance applies to all users of TEAL ICT and wi-fi, and all social networking sites, chat rooms, forums, podcasts, blogs, texting, online encyclopaedias with open access (such as Wikipedia) and content sharing sites such as YouTube. Social media can serve as a learning tool where training videos and other materials are made easily accessible to pupils 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 people vulnerable if they fail to observe a few simple precautions. Social networking websites provide an opportunity for people to communicate 'en masse' and share ideas regardless of geographical distance, however, there is the risk that posts and messages may feel private, when in fact they are in the public domain.

Safeguarding

As detailed within this policy, users must not use personal messaging to communicate with pupils. If users are unsure, they should seek advice from their line manager in the first instance. Users must not share personal contact details with pupils (mobile telephone numbers, non-work email addresses, social networking sites etc.) and any unintended breach must be reported to the IT Helpdesk and the user's line manager immediately. If users receive contact online from a pupil or ex-pupil they should decline the contact, explaining the safeguarding reasons for this, and they should notify their line manager or Designated Safeguarding Lead. Where there are genuine reasons for this type of communication, eg. clubs you manage outside of work, this should be discussed with you line manager.

Confidentiality

Disclosure of confidential information on, or via, social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- the Health and Safety at Work Act 1974
- the Data Protection Act 2018

Users should also be aware that other laws relating to libel, defamation, harassment, and copyright may apply to information posted on social media, and users can be held personally liable for breaches. Such laws include (but may not be limited to):

- the Libel Act 1843
- the Defamation Acts 1952 and 1996
- the Copyright, Designs and Patents Act 1988
- the Criminal Justice and Public Order Act 1994
- the Protection from Harassment Act 1997
- the Malicious Communications Act 1998
- the Communications Act 2003

It is crucial that users ensure they are familiar with TEAL's Data Protection Policy and this policy and that they do not breach confidentiality when using social media.

Users must not discuss confidential information relating to TEAL on their personal social media sites or accounts. Photographs, videos, or any other images which identify TEAL premises, pupils or their families, or users wearing school logos must not be placed online on any form of personal social media site. TEAL email addresses and other official contact details must not be used either for setting up personal social media accounts or for the facilitation of communication through such media.

Reputation
TEAL recognises that users are entitled to make use of social media in a personal capacity away from work. Users must be mindful that their online actions can potentially cause damage to the reputation of the organisation if they are identified as being employees of, or as having professional links to TEAL. Users must therefore ensure that if they engage with social media they must do so sensibly and responsibly. They must be confident that any content, comment, or opinion expressed through their personal use of social media will not adversely affect, nor be found damaging to, the reputation or credibility of the trust, nor otherwise breach any of TEAL's policies. Users should be aware that, in the event that they access any personal web-based email accounts via their school network, those accounts may be subject to TEAL's internet monitoring.

Users must avoid bringing TEAL into disrepute and must not use any online (or equivalent) facility to attack or abuse colleagues or pupils. Users are encouraged not to discuss their work on social media, and any views they express should be referred to as their own and not necessarily reflective of their employer's views.

Users must not edit open access online encyclopaedias (such as Wikipedia) in a personal capacity at work, as the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from TEAL.

Privacy
Users must ensure their social media accounts do not compromise their professional position and they should ensure that their privacy settings are set correctly. Users should also be aware that settings can change and they should regularly review their list of friends. Users are advised to ensure that they set the privacy levels of their personal sites securely and to opt out of public listings on social networking sites in order to safeguard their own privacy.

Users should at all times be vigilant about what may or may not legitimately be posted online, and should be aware that it is not safe to reveal home addresses, telephone numbers or other personal information online. Users are encouraged to be mindful of the risk of fraud and identity theft online and are advised to carefully consider the amount of personal information they display, share, or reveal online. Users should always keep their passwords secret and take all necessary measures to protect access to accounts.

Individuals should remember that by making use of social media they are effectively placing information within the public domain and cannot be reliant on the belief that supposedly 'private' comments or viewpoints will not gain a wider currency or exposure.

For more information about keeping your social media accounts private and general guidance about all apps, visit our TEAL safeguarding HUB:

https://theeducationalliance.onlinesafetyhub.uk/

Conduct on social networking sites
When using social media, users must not do anything that may bring TEAL into disrepute. Users are encouraged to think about any photos they may appear in and on social media (e.g. they may wish to 'untag' themselves from a photo). If users find 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.

Users are reminded that parents and pupils 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 victims of cyber-bullying, they should contact their line manager.

Users must observe all relevant copyright law before posting content that doesn’t belong to them.

Appendix of policy updates following each review

June 2024

The **ICT Acceptable Use Policy** had built up over time and had become a lengthy policy with elements that didn't flow well and some repetition. It has therefore been reduced and hopefully flows well. It aligns with safeguarding and data protection requirements and amendments are in red.