ICT & Acceptable Use Policy

Name of setting: Tigers Education Ltd

Date of policy publication: January 2025

Author/s of policy: Nicola Wharam

Date of next review: January 2026

Policy review dates and changes:

Review Date	By Whom	Summary of Changes Made	Date Implemented

Introduction and aims

Information and communications technology (ICT) is an integral part of the way our setting works, and is a critical resource for pupils, staff (including the senior leadership team), volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of Tigers Education. However, the ICT resources and facilities our setting uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of Tigers Education ICT resources for staff, pupils, parents and visitors.
- Establish clear expectations for the way all members of Tigers Education engage with each other online.
- Support Tigers Education policies on data protection, online safety and safeguarding.
- Prevent disruption that could occur to the setting through the misuse, or attempted misuse, of ICT systems.
- Support Tigers Education in teaching pupils safe and effective internet and ICT use.

This policy covers all users of Tigers Education ICT facilities, including staff, pupils, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our disciplinary procedures.

Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018.
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020.
- Computer Misuse Act 1990.
- Human Rights Act 1998.
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- Education Act 2011.
- Freedom of Information Act 2000.
- Education and Inspections Act 2006.
- Keeping Children Safe in Education 2023.
- Searching, screening and confiscation: advice for schools 2022.
- National Cyber Security Centre (NCSC): Cyber Security for Schools.
- Education and Training (Welfare of Children) Act 2021.
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- Meeting digital and technology standards in schools and colleges.

Definitions

- ICT facilities: all facilities, systems and services including but not limited to network
  infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of The setting's ICT service.
- Users: anyone authorised by Tigers Education to use the setting's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- Personal use: any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user.
- Authorised personnel: employees authorised by Tigers Education to perform systems administration and/or monitoring of the ICT facilities.
- Materials: files and data created using the setting's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

Unacceptable use

The following is considered unacceptable use of Tigers Education's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings.
Unacceptable use of Tigers Education ICT facilities includes:

- Using Tigers Education's ICT facilities to breach intellectual property rights or copyright.
- Using Tigers Education's ICT facilities to bully or harass someone else, or to promote unlawful discrimination Breaching any Tigers Education policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity Online gambling, inappropriate advertising, phishing and/or financial scams.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams Activity which defames or disparages Tigers Education, or risks bringing the setting into disrepute.
- Sharing confidential information about Tigers Education, its pupils, or other members of the setting.
- Connecting any device to the setting's ICT network without approval from authorised personnel.
- Setting up any software, applications or web services on the setting's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the setting's ICT facilities, accounts or data.

- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to Tigers Education ICT facilities.
- Causing intentional damage to the setting's ICT facilities.
- Removing, deleting or disposing of Tigers Education ICT equipment, systems, programmes or information without permission from authorised personnel.
- Causing data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to Tigers Education.
- Using websites or mechanisms to bypass the setting's filtering or monitoring mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way.

This is not an exhaustive list.

The setting reserves the right to amend this list at any time. The AP Lead will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of Tigers Education ICT facilities.

Exceptions from unacceptable use

Where the use of Tigers Education ICT facilities (on the premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the AP Lead's discretion.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with Tigers Education policies.

Access to Tigers Education ICT facilities and materials

Tigers Education manages access to the setting's ICT facilities and materials for staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices.
- Access permissions for certain programmes or files.

Staff will be provided with unique login/account information and passwords that they must use when accessing Tigers Education ICT facilities. Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the AP Lead for assistance.

Use of phones and email

Tigers Education provides each member of staff with an email address, this email account should be used for work purposes only.

- Staff should enable multi-factor authentication on their email account(s).
- All work-related business should be conducted using the email address that Tigers Education has provided.
- Staff must not share their personal email addresses with parents and pupils and must not send any work- related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents.
- Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure.
- All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email.
- Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed, and the email deleted.
- If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the AP Lead immediately and follow our data breach procedure.
- Staff must not give their personal phone number(s) to parents or pupils.
- Staff must use phones provided by Tigers Education to conduct all work-related business.
- Tigers Education phones must not be used for personal matters.
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Personal use

Staff are permitted to occasionally use Tigers Education ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. Personal use is permitted provided that such use:

- Does not take place during contact/teaching time, non-break times etc.
- Does not constitute 'unacceptable use', as defined in section 4.
- Takes place when no pupils are present.

- Does not interfere with their jobs or prevent other staff or pupils from using the facilities for work or educational purposes.
- Staff may not use the setting's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).
- Staff should be aware that use of Tigers Education ICT facilities for personal use may put personal communications within the scope of the setting's ICT monitoring activities.
- Where breaches of this policy are found, disciplinary action may be taken.
- Staff should be aware that personal use of ICT (even when not using Tigers Education ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.
- Staff should take care to follow Tigers Education guidelines on use of social media and use of email to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

The setting has guidelines for staff on appropriate security settings for Facebook accounts.

Remote access

- We allow staff to access Tigers Education ICT facilities and materials remotely.
- Staff accessing Tigers Education ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site.
- Staff must be particularly vigilant if they use Tigers Education ICT facilities outside the setting.

Tigers Education social media accounts

- Tigers Education has a range of social media accounts, managed by the Directors. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.
- Tigers Education has guidelines for what may and must not be posted on its social media accounts.
- Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.
-

Monitoring and filtering of Tigers Education network and use of ICT facilities

- To safeguard and promote the welfare of children and provide them with a safe environment to learn, the setting reserves the right to filter and monitor the use of its ICT facilities and network.
- This includes, but is not limited to, the filtering and monitoring of:
- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- Telephone calls.
- User activity/access logs.
- Any other electronic communications.
- Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.
- The effectiveness of any filtering and monitoring will be regularly reviewed.
- Where appropriate, authorised personnel may raise concerns about monitored activity with the designated safeguarding lead (DSL) and ICT manager, as appropriate.

Tigers Education monitors ICT use in order to:

- Obtain information related to Tigers Education business.
- Investigate compliance with setting policies, procedures and standards.
- Ensure effective ICT operation.
- Conduct training or quality control exercises.
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.
- The AP Lead & Directors will regularly review the effectiveness of the setting's monitoring and filtering systems.

Pupils

Access to ICT facilities

Computers and ICT facilities are available to pupils under the supervision of staff.

Unacceptable use of ICT and the internet outside of school

The setting will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the setting's policies or procedures.

- Any illegal conduct or making statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages Tigers Education, or risks bringing Tigers Education into disrepute.
- Sharing confidential information about Tigers Education, other pupils, or other members of staff.
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to Tigers Education's ICT facilities.
- Causing intentional damage to Tigers Education ICT facilities or materials.

Parent/Carers

Access to ICT facilities and materials

Parents do not have access to Tigers Education ICT facilities as a matter of course.

However, parents working for, or with, the setting in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the setting's facilities at the AP Lead's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the setting online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with Tigers Education through our website and social media channels.

We ask parents to sign the agreement as part of the induction process.

Communicating with parents about pupil activity

Tigers Education will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents in the same way that information about homework tasks

is shared. In particular, staff will let parents know which (if any) person or people from The setting pupils will be interacting with online, including the purpose of the interaction.

Parents may seek any support and advice from The setting to ensure a safe online environment is established for their child.

Data security

The setting is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts.

The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies. Staff, pupils, parents and others who use Tigers Education ICT facilities should use safe computing practices at all times.

We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls.
- Security features.
- User authentication and multi-factor authentication.
- Anti-malware software.

Passwords

All users of Tigers Education ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action.

Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

Software updates, firewalls and anti-virus software

All Tigers Education's ICT devices that support software updates, security updates and anti-virus products will have these installed and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the setting's ICT facilities.

Any personal devices using the Tigers Education network must all be configured in this

way.

Data protection

All personal data must be processed and stored in line with data protection regulations and Tigers Education's data protection policy. Please see our website for all policies.

Access to facilities and materials

All users of Tigers Education ICT facilities will have clearly defined access rights to the systems, files and devices.

These access rights are managed by the AP Lead.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access.

If access is provided in error, or if something a user should not have access to is shared with them, they should alert the AP Lead immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access.

Equipment and systems should always be logged out of and shut down completely at the end of each working day.

Encryption

Tigers Education makes sure that its devices and systems have an appropriate level of encryption.
Staff may only use personal devices (including computers and USB drives) to access setting data, work remotely, or take personal data (such as pupil information) out of the setting if they have been specifically authorised to do so by the AP Lead.

Protection from cyber attacks

Tigers Education will:

- Work with the AP Lead and the IT department to make sure cyber security is given the time and resources it needs to make the setting secure.
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the annual training window) on the basics of cyber security, including how to:
- Check the sender address in an email.
- Respond to a request for bank details, personal information or login details - Verify requests for payments or changes to information.
- Make sure staff are aware of its procedures for reporting and

responding to cyber security incidents.
- Investigate whether our IT software needs updating or replacing to be more secure.
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.

Put controls in place that are:

- Proportionate: the setting will verify this using a third-party audit to objectively test that what it has in place is effective.
- Multi-layered: everyone will be clear on what to look out for to keep our systems safe.
- Up to date: with a system in place to monitor when Tigers Education needs to update its software.
- Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be.
- Back up critical data and store these backups.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to IT support.

Make sure staff:

- Enable multi-factor authentication where they can, on things like Tigers Education email accounts.
- Make sure ICT staff conduct regular access reviews to make sure each user in the setting has the right level of permissions and admin rights.
- Have a firewall in place that is switched on.
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification.
- Develop, review and test an incident response plan with the IT department including, for example, how Tigers Education will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident.
- This plan will be reviewed and tested on a regular basis and after a significant event has occurred.

Internet access

The setting's wireless internet connection is secure, with filtering arrangements in place.

Pupils

Learners are supervised at all times when accessing the internet via the settings WIFI.

Parents and visitors

Parents and visitors to Tigers Education will not be permitted to use the Wi-Fi unless specific authorisation is granted by the AP Lead. The AP Lead will only grant authorisation if:

- Parents are working with Tigers Education in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Monitoring and review

The AP Lead will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of Tigers Education.

This policy will be reviewed annually.

Related policies

This policy should be read alongside:
E-Safety Policy.