HR

ICT Acceptable Use Policy

Staff and Trustees

The Bishop of Winchester Academy

Sapere Aude

Policy Control Table	
Policy Title	**(HR) ICT Acceptable Use Policy**
Author/s: Name, Code, Role	Catherine Watson, CWA, Director of People and Culture Sue Spencer, SSP, Network Manager Reviewed by Luke Prince, Aux IT Solutions Director
Link Trustee, if any	
Version (V) N°	1
Statutory	**Yes** ☑ **No** ☐ Internal Policy
Required on Website	**Yes** ☐ **No** ☑
Approval/Ratification Route	☐ Author – Vice principals ☐ Author - ALT - Trust Board ☑ Author - ALT - Resources Committee ☐ Author - ALT - Student Experience Committee
Review Frequency and Authority	**Vice principals (VPs)** annual ☑ biennial ☐ triennial ☐ **Trust committee** annual ☑ biennial ☐ triennial ☐ **Trust board** annual ☐ biennial ☐ triennial ☐ **Other** (state) updated if/when guidance changes ☐
Linked Policies, if any	• Staff Code of Conduct • Disciplinary Policy • Online Safety Policy
Review by Author/VPs Due	Michaelmas 2026
Pending Ratification by Committee on	Michaelmas 2026
Pending Ratification by Board on	n/a
Previous Ratification Date	n/a
Ratification Date and Authority	Resources Committee 06.11.25

A review or ratification/approval date is not a sunset clause.
The policy remains in place until such time as it has been reviewed, re-ratified/approved or superseded by updated relevant statutory guidance.

Policy History			
V	**Date**	**Author**	**Revision Summary**
1	Michaelmas 2025	CWA/SSP	S7: New section about physical security of devices. S8: addition of 8.2-8.3 re anti-virus requirements and compromise protocol. 4.3 Insertion on the expectations of the use of LinkedIn for professional networking and expected protocols to protect the academy's reputation.

Contents

Sponsors' Statement

All The Bishop of Winchester Academy (TBOWA) policies exist to support the Sponsors' vision, Christian ethos and values that are embedded in the day-to-day and long-term running of the academy. Each policy evidences the commitment of the Sponsors to the principles and values of honesty, respect, hospitality, compassion, love, forgiveness, self-discipline, creativity and hope. This policy contributes to the development of young people and the community through all Academy activities.

1. Policy Statement

1.1. ICT is provided to support and improve the teaching and learning in the academy as well as ensuring the smooth operation of our administrative and financial systems. We aim to ensure users of the academy's ICT use it safely, operating within legal andstatutory frameworks, expectations, our culture and ethos.

2. Scope

2.1 This policy applies to all employees, workers, supply staff, volunteers, trustees and others accessing ICT at TBOWA and they will be termed as 'users' within this policy, and it details the academy's expectations of all users of TBOWA's electronic communication, including, but not limited to telephone, social media platforms, email, internet, and ICT systems.

2.2 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 TBOWA ICT, this also includes any academy specific facilities, equipment, and networks. This policy still applies when users access any of TBOWA's systems off-site.

2.3 By using TBOWA's provision, or using personal devices onsite, all users are agreeing to adhere to this policy.

2.4 Any failure to comply with this policy may be managed through the disciplinary procedure. If we are required to investigate a breach of this policy, you will be required to share relevant password and login details.

3. Roles and responsibilities

3.1 The **Principal** is responsible for ensuring that leaders, staff and users are aware of and adhere to this policy and procedure and that breaches are managed swiftly, effectively, fairly, and consistently.

3.2 **IT Support** is responsible for ensuring that all employees understand their responsibilities when using ICT at work and that systems are used and managed effectively. IT Support 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 Principal or a member of the Academy Leadership Team (ALT).

3.3 All users must ensure they **report any breaches of this policy immediately to IT Support at support@tbowa.org** , the Principal or ALT. Data protection breaches must be logged on the Data Breach Form on the Academy's intranet. Any serious breaches should also be reported immediately to the Academy's Data Protection Officer.

3.4 All **users** must ensure they understand and adhere to TBOWA'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 IT Support.

4. Key principles

4.1 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 the academy guard itself from cyber-attacks and data breaches.

4.2 Users are asked not to identify themselves with The Bishop of Winchester Academy 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.

4.3 When users are using Linked In for professional networking purposes, reference may be made to The Bishop of Winchester Academy as their employer, but appropriate content and messaging must be adhered to when using this platform to ensure that there is no reputational harm to the academy.

4.4 When using ICT for work purposes, users must not:

- Act in a way that contravenes the Academy's Code of Conduct and other academy policies, legislative, statutory, or professional requirements.
- Disclose sensitive information or personal data to unapproved people or organisations.
- Breach the Academy'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 principal (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 IT support at support@tbowa.org 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 the academy's expectations.

4.5 If a user accidentally accesses inappropriate material on the internet or by email, they must contact IT Support and the DSL.

4.6 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 the academy's wi-fi, which would be viewed inappropriate. Under no circumstances should any users download, upload, or bring into the academy, 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 IT Support.

4.7 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 the academy's 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 the academy's equipment by employees at home (e.g. laptops and tablets).

4.8 Users must not 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 IT Support and the user's line manager immediately.

4.9 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.

4.10 Users are advised (e.g. through briefings) that internet-based activity on personal devices is monitored and logged whilst using the academy's wi-fi, and misuse of the academy's ICT systems and networks may breach the TBOWA's Code of Conduct, other policies and/or proceduresand/or the law. Any attempt by a user to compromise the security or functionality of the academy's networks and its ICT systems, either internally or externally, will be considered as "hacking". It should be notedthat "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 the academy'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.

4.11 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 the academy's ICT systems. This includes, but is not exclusive to:

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

4.12 Any breach of copyright whilst using the academy's ICT systems is the individual user's responsibility and TBOWAcannot accept any liability or litigation for such a breach.

4.13 Users must ensure that:

- Personal mobile phones and laptops or school IT equipment are not used for personal use in school hours or in front of students.
- Personal mobile phones or cameras are not used to take pictures of students.
- They keep personal data safe, taking steps to minimise the risk of loss or misuse of data.
- Before leaving a computer for any length of time, users must log off the network or lock the computer, checking that the logging off procedure is complete before you leave.
- 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 TBOWA's Data Protection Policy and associated procedures and guidelines.

4.14 Users should ensure:

- personal email and texts should only take place before or after working hours or during breaks.
- use of the internet at work does not interfere with the efficient performance of your role.
- they log out of their computers at the end of the day.
- ensure that their messages are relevant and appropriate to targeted recipients (e.g. not using 'blanket' or 'all-user' emails)
- they 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.

- email and electronic communication does not replace face to face communication.

We reserve the right to remove internet access for any employee at work.

4.15 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 the academy has requested that use cease because it is causing disruption to the correct functioning of TBOWA's ICT systems and/or networks
- unauthorised monitoring of data or traffic on the academy's ICT network or systems without the express authorisation of the owner of the network or systems.

5. Email and electronic communication acceptable use

5.1 When using academy 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 academy 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 considerationshould always be taken before sending an email (e.g. freedom of information requests and subject access requests).

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

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

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

6. Viruses and Malware

6.1 Viruses and malware can expose TBOWA to very considerable risks. You are required to take all reasonable steps to avoid the introduction of any virus or malware on TBOWA equipment, systems, or networks.

6.2 Reasonable steps will include, but are not limited to:

- Ensuring that files downloaded from the internet, received via email or on removable media such as a memory stick are checked for any viruses using TBOWA provided anti-virus software before being used;
- Not using any removable media, such as a memory stick, unless encrypted and with prior approval from authorised ICT staff;
- Being cautious when opening any emails that you are not expecting especially those that contain an attachment or web link;
- Not following any links to questionnaires, offers, requests, etc. from unknown sources or emails that you are not expecting - delete the email and flag it with a member of IT staff
- Not forwarding any suspect emails to anybody other than if requested by a member of IT staff: Delete it.
- Not forwarding any suspect emails to anybody, other than if requested by a member of IT staff: Delete it; delete emails with attachments that you were not expecting even if you think you know the person sending, if the wording seems "odd" in some way. Adversaries can often spoof the Sender field in emails to make it look like someone you know is emailing you;

- Not installing any hardware or software without the express permission of the relevant ICT staff;
- Allowing any anti-virus software to be installed on TBOWA ICT equipment and software updates.
- Ensuring that any ICT equipment provided by TBOWA for use off site, benefits from regular TBOWA anti-virus updates either by using it to log onto the relevant networks and allowing the updates to run or by providing it to the IT support so that such updates can be undertaken.

6.3 If you suspect there may be a virus or malware on any TBOWA ICT equipment, you must stop using the equipment and contact IT Support immediately for further advice.

6.4 Report any attempted phishing e-mail to IT Support in order that they can make sure that investigations can be made into potential other users receiving the email. Often a phishing e-mail is sent to a number of people.

7. Physical security of devices borrowed or removed from site

7.1 Staff, or trustees, issued with Academy devices must ensure their physical security on-site, off-site, and in transit. Reasonable steps must be taken to prevent damage, loss, or theft (e.g. keeping devices out of sight). Never leave devices in unsecured locations, such as in view within vehicles or public areas. Any loss, theft or damage must be reported immediately to support@tbowa.org

8. Remote access, including from home and other venues

8.1 Remote working and access is covered by this policy in the same way as access to TBOWA equipment at the Academy. It is your responsibility to retain securely all passwords, fobs, and any other devices necessary for remote access. Particular care must be taken when accessing systems remotely in a public space or private spaces that are shared areas to ensure that screens cannot be viewed by others. You must ensure your actions are compliant with relevant legislation when accessing systems remotely.

8.2 Devices used for remote desktop access, must be up-to-date and protected by current, active anti-virus. If access occurs from a device suspected of compromise or infection, this must be reported immediately support@tbowa.org.

8.3 Where the remote desktop is an entrance into school systems, users must have an additional device to enable them to report the compromise to support@tbowa.org.

8.4 Where available, all remote access to systems and cloud-based systems should be secured using multi factor authentication (MFA).

9. Monitoring

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

9.2 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 the academy's 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.

10. Passwords

10.1 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.

10.2 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 the academy's networks. Users should change their password each term, and passwords should have:

- Have a minimum of eight 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, !, $, #, %)

11. Monitoring compliance with effectiveness of the policy

11.1 Effectiveness and compliance of this policy will be regularly monitored by the Academy's Leadership Team.

12. Appendix 1: Social Media Guidance

1. Introduction

1.1 This guidance applies to all users of the academy's ICT and wi-fi, and all social networking sites, chat rooms, forums, podcasts, blogs, texting, online encyclopedias 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 the academy 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 peoplevulnerable 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.

2. Safeguarding

2.1 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 IT support 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, e.g. clubs you manage outside of work, this should be discussed with you line manager.

3. Confidentiality

3.1 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

3.2 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

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

3.4 Users must not discuss confidential information relating to the Bishop of Winchester Academy on their personal social media sites or accounts. Photographs, videos, or any other images which identify the academy's premises, pupils or their families, or users wearing school logos must not be placed online on any form of personal social media site.

3.5 TBOWA 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.

4. Reputation

4.1 TBOWA 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 academy if they are identified as being employees of, or as having professional links to the academy. 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 TBOWA's policies. Users should be aware that, in the event that they access any personal web-based email accounts via their academy network, those accounts may be subject to TBOWA's internet monitoring.

4.2 Users must avoid bringing TBOWA 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.

4.3 Users must not edit open access online encyclopedias (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 the academy.

5. Privacy

5.1 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.

5.2 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.

5.3 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.

6. Conduct on social networking sites

6.1 When using social media, users must not do anything that may bring TBOWA 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.

6.2 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 academy.

6.3 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.

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