



POLICY	ICT Acceptable Use Staff
STATUS/DATE OF THIS VERSION	July 2026
APPROVED BY	Board of Trustees
RATIFIED BY	Board of Trustees – July 2026
REVIEW	July 2027

This policy is operated by all the schools in Unity Education Trust (as listed below). **There may be sections that are specific to one school and these will be added by the school either as an annex or in place of yellow highlighted sections below.**

Any queries about the policy should be directed, in the first instance, to the Headteacher/Head of School:

- **Beeston Primary**
- **Garvestone Primary**
- **Grove House Infant**
- **Kings Park Infant**
- **Northgate High School and Dereham Sixth Form College**
- **The Pinetree School**
- **Churchill Park**
- **Greyfriars Primary**
- **Highgate Infant School**
- **Kings Oak Infant School**
- **Wimbotsham and Stow Primary**
- **Magdalen Primary**
- **St Germans Primary**
- **Great Dunham Primary**
- **UET Compass Belton Academy**
- **UET Pathfinder Douglas Bader Academy**

Acceptable Use Policy Agreement (Staff)

Technology is now entwined in our modern lives with everyday use of social media and web-based communication a standard practice. It is therefore important to ensure good awareness both of the possibilities to learn, create and share ideas and also the risks that these freedoms bring both to the welfare of staff and students and to the integrity of the IT systems that the school relies on to provide learning and teaching.

All users accessing our school systems should be entitled to safe access to the internet and IT systems at all times. This policy is intended to provide a working framework for staff to uphold the positive ideals of the technology we use while providing a safe learning environment and protecting the data we manage in the course of our services to students and their families.

The policy will outline how:

- Staff must ensure they are responsible users of the IT systems provided and that they make sound judgements while using the internet and other communications technologies for educational and personal use.
- The school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff can ensure they are protected from potential risk in their use of technology for educational and personal use.

Schools AUP Agreement:

I agree that I must use school IT systems in a responsible way. I must do so to ensure there is no risk either to my own safety or to the safety and security of the students and school IT systems. I will, where possible, guide students in the safe use of technology with a strong focus on safe and responsible use of the internet and online services.

For the purposes of safeguarding and security:

- I understand that the school will monitor my use of the school IT and communications systems.
- I understand the rules in this document apply equally to the use of school and personal devices and systems (e.g. laptops, email, VLE etc.) outside of school

- I understand the importance of appropriate controls on the transfer and sharing of personal data (digital or paper-based) out of school. Encryption and file transfer receipts.
- I understand that the school IT systems are primarily intended for educational use.
- I will only use the systems for personal or recreational use when appropriate.
- I will never disclose my username or password to anyone else, nor use any other person's username and password to access systems not provided to me.
- I understand that I should not record any password where it is possible that someone may view it or steal it.
- I will immediately report any incident or activity I am aware of which may be illegal, inappropriate or present risk to the school or individuals to Headteacher.

I will use all the school IT and communication systems professionally. In doing so:

- I will not access, copy, alter, share or delete any other user's files, without their express permission.
- I will communicate with others in a courteous and professional manner and refrain from any use of aggressive or inappropriate language. I acknowledge that overuse of capitalisation in an email may be misinterpreted as shouting.
- I will ensure that, if I wish to take or publish images of others, I will check that appropriate consent is recorded by the school in lines with the school's digital media policy.
- I will only use school provided and managed equipment to record these images unless I have explicit permission to do otherwise.
- I will ensure that any published photos do not identify individuals by name or show other personal information and that photos and images are only used on a school approved and controlled platform.
- I will only communicate with students and parents/carers using provided school IT systems. All communication will be professional in tone and manner.
- I will ensure that I do not share my personal contact information and only ever use contact details provided by the school.
- I will not engage in any online activity that may compromise my professional integrity or provide a risk to the students, my colleagues, the school IT systems or myself.

The school and the Trust will provide safe and secure access to school IT systems and services and maintain the availability and integrity of the school systems in support of learning and teaching. However, any use of personal mobile devices (such as but not limited to, laptops/tablets/ mobile phones) in school, must be in accordance with rules set out in this agreement, as per any school managed equipment.

Staff members must:

- Configure multifactor authentication on systems and services as required.
- Only use generative AI tools as instructed and in line with the Trust AI policy.
- Ensure that any such personal devices are protected by up-to-date security patches and anti-virus software and are free from viruses.
- Remain vigilant when accessing emails. Never click on any hyperlinks in emails or any attachments to emails, unless the sender is known and trusted.
- Report concerns regarding emails or communication received on any other school or personal IT system must be flagged to the Data and Systems Lead.
- Report concerns in relation to suspected hacking or phishing attempts on school or personal IT systems must be reported immediately to the Data and Systems Lead.
- Store work in the appropriate, provided, locations on the school network or systems to guarantee appropriate levels of backup and malware scanning.
- Not try to upload, download or access any materials which are illegal (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.
- Not try to use any applications, such as VPN, that might allow them to bypass the filtering/security systems in place to provide a safe learning and teaching environment.
- Not install any applications on school devices without consultation and support from the Data and Systems Lead. Neither should they change settings put in place by the school to ensure appropriately managed devices.
- Report any damage to or faults in school equipment.
- Only share personal information collected and managed by the school with others as their role permits or when required by law or by school policy to disclose such information to an appropriate authority. Any data sharing must be by approved and encrypted communication services provide by the school or their business partners.
- When travelling, place laptops/phones/tablets in the boot of their car.
- Ensure that ICT equipment provided by the Trust is stored securely when not in use, e.g., not leaving devices on show in the home or vehicle when

unoccupied. If lost or stolen, the headteacher must be provided with a police crime number.

- Ensure that copyright resources are only used or shared with appropriate permissions. Copyrighted work will not be downloaded or shared including music and videos unless an exemption applies for teaching purposes.
- These purposes include:
 - the copying of works in any medium as long as the use is solely to illustrate a point, it is not done for commercial purposes, it is accompanied by a sufficient acknowledgement, and the use is fair dealing. This means minor uses, such as displaying a few lines of poetry on an interactive whiteboard, are permitted, but uses which would undermine sales of teaching materials are not;
 - performing, playing or showing copyright works in a school, university or another educational establishment for educational purposes. However, it only applies if the audience is limited to teachers, pupils and others directly connected with the activities of the establishment. It will not generally apply if parents are in the audience. Examples of this are showing a video for English or drama lessons and the teaching of music. It is unlikely to include the playing of a video during a wet playtime purely to amuse the children;
 - by recording a TV programme or radio broadcast for non-commercial educational purposes in an educational establishment, provided there is no licensing scheme in place. Generally, a licence will be required from the Educational Recording Agency;
 - making copies by using a photocopier, or similar device on behalf of an educational establishment for the purpose of non-commercial instruction provided that there is no licensing scheme in place. Generally, a licence will be required from the Copyright Licensing Agency.

These and other, exemptions to copyright are listed here:

<https://www.gov.uk/guidance/exceptions-to-copyright>

I have read and understood the above and agree that:

- I am responsibly upholding the requirements laid out above at all times and that even while in personal time I am representing the values and integrity of the school.
- This Acceptable Use Policy applies not only to my work and use of school provided IT equipment but also applies to my use of school IT systems.
- If I fail to comply with this Acceptable Use Policy Agreement, I understand that I may be subject to disciplinary action as per the terms laid out in the school's Disciplinary Policy.

Name:	
Signed:	
Date:	