

	Name of School	Cranbrook Primary School
	AUP review Date	November 2025
	Date of next Review	November 2026
	Who reviewed this AUP?	DPO and SBM

Acceptable Use Policy (AUP): Staff and Governors Agreement Form

This agreement covers the use of digital technologies in school — including email, the Internet, intranet and network resources, learning platforms, software, equipment, and systems.

Agreement

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed *reasonable* by the Headteacher and Governing Body.
- I will undertake regular cyber security training, such as the **Cyber Security Training for School Staff** provided by the National Cyber Security Centre (NCSC): www.ncsc.gov.uk/information/cyber-security-training-schools
- I will not reveal my password(s) to anyone.
- My passwords will contain at least 8 characters and preferably 15 characters, comprising lowercase letters, capital letters, numbers, and symbols.
- I will not click on email links from untrusted sources.
- I will not print personal data in a location where it could be compromised.
- I will communicate professionally when using school email and communication systems. I understand that information may be disclosed to any person(s) referred to within the communication.
- I will keep data secure by locking away documentation, speaking about personal data only in a secure environment (out of earshot of others), setting computers to time out, and password-protecting or encrypting data when communicating externally. This includes when working from home or outside the school premises.
- I will not allow unauthorised individuals to access email, the Internet, the intranet, the network, or other school or local authority systems.
- I will not download or save sensitive or personal data onto a personal device. Such data will only be stored on the school server and/or school devices.
- I will only use my own devices if permission has been granted by the SLT. I will ensure that appropriate anti-virus software is installed and that suitable security measures (e.g. two-factor authentication) are in place.
- I will ensure that I work in a secure environment where my screen is not visible to others when handling sensitive or personal data.
- I will always log out when I finish working.
- I will report any data breaches to the SLT or Data Protection Officer as soon as possible.

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will respect school Wi-Fi protocols if using a personal device and will not visit social media or inappropriate websites.
- I will not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.
- I will not take secret recordings or screenshots of myself or pupils during live lessons.
- I will conduct any video lessons in a professional environment, as if I were in school. This means I will be appropriately dressed and not in a visible bedroom environment. If unavoidable, I will ensure that the background does not reveal any personal information or inappropriate content and, where possible, I will use a blurred or virtual background.
- I will only use the approved, secure school email system(s) for any confidential school business.
- I will only use approved school email or other school-authorised communication systems when communicating with pupils or parents/carers, and only on appropriate school business. I will not use my personal phone to communicate with parents without prior approval from the Headteacher, except in an emergency, and I will withhold my number if doing so.
- I will not browse, download, or send material that could be considered offensive.
- I will report any accidental access to or receipt of inappropriate materials, or any filtering breach, to the ICT Team.
- I will not click on links, or download software or resources from the Internet that could compromise the network or are not adequately licensed.
- I will not connect a computer, laptop, or other device (including USB flash drives) that does not have up-to-date anti-virus software to the school network or Internet. I will keep any loaned equipment up to date using the school's recommended anti-virus, firewall, and ICT security systems.
- I will not use personal digital cameras, tablets, laptops, or other devices for taking or transferring images of pupils or staff without permission, and I will not store images without the consent of the data subjects.
- I will not use a personal mobile phone or any personal photographic equipment to take pictures of children.
- I will ensure that I secure ICT hardware using appropriate safety measures:
 1. My class laptop will be secured at all times.
 2. Laptops/netbooks used by pupils will be locked away in a secure cupboard at the end of each school day.
 3. Other items of ICT hardware (e.g. cameras) will be secured in lockable cupboards when not in use.
 4. I will not leave devices containing school data in my car or other forms of transport, even if locked.
- I will use cloud systems in accordance with school advice.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any *significant personal use*.
- I will only use school hardware, software, and email for business purposes and any personal use will be reasonable and responsible, minimising the risk of data breaches. I understand that any breaches may result in disciplinary procedures in line with the Staff Code of Conduct and Online Safety Policy.
- I will ensure that any confidential data I need to transport from one location to another is protected by encryption, and that I follow school data security protocols when using such data in any location.

- I understand that the Data Protection Policy requires that any information I see regarding staff or pupil information, held within the school's information management system, must be kept private and confidential — except where I am required by law to disclose such information to an appropriate authority.
 - I will embed the school's online safety curriculum into my teaching.
 - I will only use LA systems in accordance with corporate policies.
 - I understand that all Internet and network usage can be logged, and this information may be made available to the Headteacher.
-

Within Social Networking

- I will not contact pupils using social media or any other means not authorised by the school.
 - I understand that if any of my online activity affects pupils, staff, or the wider school community, this could lead to disciplinary action.
 - I will ensure that any private social networking sites, blogs, or other platforms that I create or contribute to are not confused with my professional role.
 - I understand that I must not publish any content that could result in defamation, discrimination, breaches of copyright, data protection, or any other claims for damages. This includes, but is not limited to, material of an illegal, sexual, or offensive nature that could bring the school into disrepute.
 - I will not use social networking sites for promoting personal financial interests, commercial ventures, or personal campaigns.
 - I will not breach any of the school's policies.
 - I will not discuss or post about school events, staff, or pupils without prior permission from the Headteacher.
 - I will not identify myself as a representative of the school on personal social media accounts.
-

Acknowledgement

I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature: _____

Name: _____

Date: _____

I understand that it is my responsibility to remain up to date with the school's online safety and data protection policies.

I agree to abide by all the points above and request access to the school's ICT resources and systems, including an email/computer account.