

	Name of School	Cranbrook Primary School
	AUP review Date	November 2024
	Date of next Review	November 2025
	Who reviewed this AUP?	DPO and SBM

Acceptable Use Policy (AUP): Staff and Governors agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- 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 [Cyber security training for school staff - NCSC.GOV.UK](https://www.ncsc.gov.uk/information/cyber-security-training-schools) <https://www.ncsc.gov.uk/information/cyber-security-training-schools>
- I will not reveal my password(s) to anyone
- Passwords will be of at least 8 characters and preferably 15 characters. comprising small letters, capital letters, numbers and symbols
- I will not click on email links from untrusted sources
- I will not print personal data to a location where it can be compromised
- I will communicate professionally when communicating internally whilst using school email and communication systems. I understand that information can be disclosed to person(s) that are referred to within the communication.
- I will keep data secure by locking away documentation, speaking about personal data in a secure environment which is out of the earshot of others, setting computers to time out, password protecting and encrypting when communicating externally etc. This includes working from home and or outside the school.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will not download or save sensitive or personal data onto a personal device, I will store this data on the school server and or school devices.
- I will only use my own devices if permission is given by the SLT. I will ensure that appropriate anti-virus software is installed, and appropriate security measures are in place. E.g., dual factor authentication.
- I will ensure that I work in a secure environment where my screen is not visible to others when working on sensitive or personal data.
- I will always log out when I finish working.

- I will report any data breaches to the SLT/ 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 if using a personal device and will not visit social media and 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 with 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 am in school. This means I will be correctly dressed and not in a bedroom, or impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
- I will only use the approved, secure email system(s) for any confidential school business.
- I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business. I will not use my own phone to communicate with parents without prior approval of the Headteacher except in an emergency and I will withhold my number.
- 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 filtering breach to the ICT Team
- I will not click on links, download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive) that does not have up-to-date anti-virus software to the network / Internet and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras, tablets, laptops or other equipment for taking and transferring images of pupils or staff without permission and will not store images without consent of the data subjects.
- I will not use a mobile phone or other photographing equipment of my own to take any 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 children 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 and or other transportation, 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 personal purposes in a responsible way which minimises the risk of any data breaches. I understand that I will be subject to disciplinary procedures in line with our staff code of conduct and online safety policy should any breaches occur.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school’s information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that 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 any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to the Head teacher.

Within Social Networking:

- I will not contact pupils using social media or any other means not authorised by the school
- If any of my online activity affects students, staff or the wider community I understand that this could lead to disciplinary action
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I understand that I cannot publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- I will not use Social Networking sites for the promotion of personal financial interests, commercial ventures or personal campaigns
- I will not breach any of the school’s policies
- I will not discuss or advise any matters relating to school events or matters, staff or pupils without prior permission from the Headteacher
- I will not identify myself as a representative of the school

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

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

I agree to abide by all the points above.

I wish to have an email/computer account and be able to use the school's ICT resources and systems.

Signature _____ Date:

Full Name _____ (printed)

Role within the school
