NEW SEAHAM ACADEMY

Staff ICT Acceptable Use Policy 2026

As a professional organisation with responsibility for safeguarding children, the school requires all staff to take appropriate measures to protect children, personal data and information systems from unauthorised access, damage, loss, abuse, manipulation and theft. All staff must use school and personal technology - including mobile and smart devices, social media, cloud services and generative AI - in a professional, lawful, secure and ethical manner. Staff are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1) I understand that information systems and ICT include networks, data and storage, online and offline communications, cloud services, filtering and monitoring systems, generative AI and access devices. Devices include computers, mobile phones, tablets, cameras, smartwatches and other connected or smart technology.

2) School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3) Mobile and smart technology (including mobile phones, smartwatches and tablets). Staff use must comply with the school's mobile phone policy and model a mobile phone-free environment for pupils by default.

   a) {Staff mobile phones will be on silent or switched off and stored securely during the school day and may only be used when children are not present (i.e. staff room)

   b) {Staff mobile phones will never be used for any reason when children are present

   c) {Staff mobile phones are allowed in school, but are not allowed to be used in sensitive areas (EYFS, cloak rooms, toilets, when children are changing, swimming). Mobile phones should only be used for communication when not working with children. Mobile phones should not be visible to pupils unless their use is linked to learning, for instance as a stopwatch or to play music.

   d) Smartwatches and other wearable/connected devices - the school's policy is all smartwatches and similar technology are not allowed in school.

   e) Cameras, audio recorders or video functions on personal devices will not be used to record pupils in any circumstances. Only school-approved devices, accounts and storage may be used where recording is authorised.

   f) Where direct contact with a parent/carer is necessary, staff will use a school-issued device, number or approved communication system; personal contact details will not be disclosed.

4) I understand that any hardware and software provided by my school for staff use can only be used by members of staff and can only be used for school related work.

5) Personal use of school ICT systems and connectivity is Not Permitted.

6) To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

7) I will protect accounts using unique passwords or passphrases that meet the school's current security standard, use multi-factor authentication where provided, keep authentication codes and recovery information confidential, and never approve an unexpected sign-in request. I will not share accounts or allow another person to use my credentials.

8) I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

9) Data protection and information security {see also the school Data Protection Policy}

   a) I will handle personal data in accordance with the Data Protection Act 2018, UK GDPR, the Data (Use and Access) Act 2025 and school policy. I will use personal data only for an authorised purpose and lawful basis; use the minimum necessary; keep it accurate, secure and no longer than required; and report any actual or suspected loss, disclosure or breach immediately. Portable storage or transfer will use only school-approved encrypted devices, accounts and services.

   b) If the school permits me to access work email or systems on a personal device, I will follow the school's bring-your-own-device arrangements, protect the device with a secure PIN/password and current security updates, prevent access by others, and ensure school data is securely removed when access ends or the device is disposed of.

   c) I will not send safeguarding information, medical information, education, health and care plans (EHCPs), or other special-category or sensitive data to a personal account or through an unapproved service. Any authorised transfer will use the school's approved secure method and only the minimum necessary information.

   d) I will not keep professional documents which contain school-related personal information (including images, files, videos etc.) on any personally owned devices (such as laptops, digital cameras, mobile phones)

   e) Images, video or audio of pupils will be created only for an authorised school purpose, using approved equipment, accounts, consent/lawful-basis arrangements and storage. They will not be transferred to personal devices or unapproved services: [insert the school's approved arrangements].

   f) I will not upload, copy or store personal data, confidential school information, pupil work, images, video or audio in unapproved cloud storage, apps, websites or generative AI services.

10) I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

11) I will respect copyright and intellectual property rights.

12) Social Media:

   a) I have read and understood the school's online safety policy, including the four areas of online risk (content, contact, conduct and commerce), the safe use of devices and social media, and the arrangements for filtering and monitoring.

   b) I will not communicate with pupils or ex-pupils using social media without the express permission of the Headteacher. *{Some schools may use social media to communicate directly with pupils, in this instance staff should use a social media account that is purely used*

for work purposes. They should complete a risk assessment to ensure that both staff and pupils are protected.}

c) My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team. *This would include any relatives of current pupils that are my "friends" on a social media site.*

d) My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

e) I will not create, request, transmit, display, publish or forward material that is abusive, discriminatory, sexualised, misleading, defamatory, harassing or likely to cause harm or needless distress, or that could bring my professional role, the school or the local authority/trust into disrepute. This applies even where material is believed to be private, temporary, deleted, AI-generated or digitally altered.

f) Generative artificial intelligence (AI) and automated tools.

g) I will use only school-approved AI tools, accounts and purposes. I will not enter personal data, safeguarding information, confidential material, pupil work, photographs, audio or video unless the school has explicitly approved the tool and use following data-protection and safeguarding assessment.

h) I remain professionally responsible for any AI-assisted work. I will check outputs for accuracy, bias, suitability, copyright and safeguarding risks, clearly identify AI use where required, and will not delegate safeguarding decisions or professional judgement to an AI system.

i) I will not use AI to create, alter or share sexualised, nude or semi-nude imagery, impersonations, deepfakes or other harmful content involving a child or colleague. I will preserve evidence and report any such content immediately through the school's safeguarding procedure without copying or forwarding it unnecessarily.

j) I will follow the school's AI, assessment, intellectual-property and information-security rules and seek advice before using an AI tool where its approval or risks are unclear.

13) I will report concerns about a child's online safety, including content, contact, conduct or commerce risks; making or sharing nudes or semi-nudes (including AI-generated or digitally altered images); cybercrime; sexual extortion; harmful sexual behaviour; filtering/monitoring concerns; or inappropriate use of technology, to the DSL [name] or deputy as soon as possible and record the concern in accordance with school procedure. If a child is in immediate danger, emergency procedures will be followed without delay.

14) I will not disable, test without authorisation, or attempt to bypass filtering, monitoring, access controls or other security systems. I will report accidental access to inappropriate material, filtering or monitoring gaps, malware, phishing, loss of a device or data, or any suspected cyber incident immediately to the DSL [name], the senior leader responsible for filtering and monitoring [name], and/or IT support [named contact], in line with the school's reporting route.

15) If I have a concern about the use of technology or online behaviour by a staff member, supply teacher, trainee teacher, volunteer or contractor, I will follow the staff behaviour/code of conduct and safeguarding procedures immediately. I will report allegations that may meet the harm threshold to the headteacher (or to the chair of governors/trustees where the concern is about the headteacher) and report low-level concerns through the school's specified route. I will not investigate the matter myself.

16) I will promote online safety with pupils through my teaching, supervision and professional example, in line with the curriculum, safeguarding policy and the school's mobile phone expectations.

17) If I have any questions about safe and professional online practice, in school or off site, I will seek advice from the DSL [name], deputy DSL or the appropriate senior leader before acting.

18) I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The school may lawfully and proportionately monitor use of its information systems, devices, networks, internet access, AI services and communications to protect children, information and systems and to check compliance with this AUP and related policies. Suspected unauthorised, unsafe or unlawful use may be addressed under safeguarding, disciplinary, data-breach or cyber-incident procedures and, where appropriate, referred to the local authority designated officer (LADO), police or another relevant agency.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy 2026 and the related school policies and reporting procedures.

Signed: ……..…….... Print Name: …… Date: ……..…

Accepted by: ……. Print Name: …….