



Independence Safe and Settled Resilience Respect Aspiration Learning Community

OUR MISSION

As an outstanding school we will inspire children to achieve more than
they ever believed possible

OUR VISION

That every member of our school community is challenged and supported
to be the very best they can be

That through our high-quality learning experiences & curriculum we will improve the
life-chances of our children. That we educate the whole child so they can thrive in a changing world

Staff Acceptable Use Policy 2025-2026

As a professional organisation with responsibility for children's safeguarding it is important that all staff take every possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse, and theft. All members of staff have a responsibility to use the school's computer systems, in whichever way this is accessed, in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they 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 school policies, relevant national and local guidance and expectations, and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email, and social media sites.
- 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.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my screen as appropriate.
- I will respect system security, and I will not disclose any password or security information. I will use a 'strong' password, (A strong password has numbers, letters, and symbols, with 8 or more characters), that does not contain a dictionary word and is only used on one system.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware, without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g., via VPN).

Free public Wi-Fi should not under any circumstances be used to access school data!

- Any data which is being removed from the school site (such as via email or on memory sticks or media) will be encrypted by a method approved by the school.
- Any images or videos of pupils will only be taken and used as stated in the school image use policy and will always take parental consent into account.

I will not discuss details concerning any pupil with colleagues with-in earshot of other pupils or with any member of my family or friends.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones). I will only view such data if the device is suitably secured and encrypted. Where possible I will use the current School Cloud Platform to upload any work documents and files in a password protected environment or via VPN. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.

I have read and understood the school Online Safety, Mobile and Smart Technology and Social Media policies, which cover the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead, **Claire Whichcord**, and/or the Online Safety Officer, **Graham Clayson (a Deputy DSL)**, as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead, **Claire Whichcord**, and/or the designated lead for filtering, **Graham Clayson**, as soon as possible.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the Head Teacher, **Claire Whichcord**, and/or my line manager as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals, will only take place within clear and explicit professional boundaries and will always be transparent and open to scrutiny. All communication will take place via school approved communication channels, e.g., a school provided email address or telephone number and not via personal communication channels, e.g., personal email or, social networking. Any pre-existing relationships or situations that may compromise this, will be discussed with the Head Teacher and/or other members of the Senior Leadership Team.
- If I use my own personal device to access school data including emails, e.g., from a mobile telephone or tablet, I will use a two-step verification e.g., fingerprint and a six-digit PIN number. If the device is lost, missing, or stolen I agree to report this to the Head Teacher immediately.
- I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming, web publications, and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and Internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school's AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school or the Coastal Academies Trust into disrepute.
- I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead, **Claire Whichcord**, and/or the Online Safety Officer, **Graham Clayson (a Deputy DSL)**.
- I understand that my use of the information systems, Internet and email will be monitored and recorded to ensure policy compliance. The school may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails to monitor compliance with this Acceptable Use Policy and the school's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the school suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

Signed:

Name:

Date: