Coastal Academies Trust

Staff Acceptable Use Policy 2022

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all 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**.**

- I will use ICT in line with the local school's procedures, risk assessments and guidance.

- 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 login as appropriate.

- I will respect system security and I will not disclose any password or security information and will use a 'strong' password (A strong password either has numbers, letters and symbols, with 8 or more characters, or is a multi word phrase.) It must only be used on one system and is changed at least once a term.

- 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 GDPR. Staff must familiarise themselves with the schools Data protection policies. Any images or videos of pupils will only be taken and used as stated in the school image use policy and will always take into account parental consent.

- I will not keep or access 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), unless they are suitably secured and encrypted. 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 e-Safety policy which covers 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, and/or the Data Protection Lead, as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead, and/or the Data Protection lead**,** 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 ICT Manager, 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 be transparent and open to scrutiny at all times. 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 member of the Senior Leadership Team.

- If I use my own personal device to access school data including emails, i.e. from a mobile telephone or Ipad, I will ensure that I use a complex password and or fingerprint or similar. If the device is lost, missing or stolen, I will change my email password and report this to the Head Teacher and IT 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 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.

- I understand that all school-related information produced, collected and/or processed in the course of schools business remains the property of the school. This includes such information stored on approved third-party servers, websites and social networking sites, such as LinkedIn.

- I understand that no information assets belonging to the school may be removed from school premises without the direct approval of the school.

- I understand that school email addresses must only be used to create login accounts for school related activities and must not be used for social media, shopping, entertainment sites etc.

- If I have any queries or questions regarding safe and professional practice online either in school or off site, then I will raise them with the **Designated Safeguarding Lead,** and/or the **Data Protection Lead or DPO**.

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

The School may exercise its right to monitor the use of ~~i~~nformation systems, including Internet access and the interception of e-mails in order 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.

This policy should be read in conjunction with:

- Child Protection Policy
- GDPR/Data Protection Policy
- Local school risk assessments e.g. Video lessons risk assessment.