Acceptable User Policy for IT (AUP)

Overview

At Coast Academies we recognise that information and communication technology play an important part in learning. All learners in school must use technology appropriately, safely and legally. We have a responsibility to make all learners aware of the appropriate behaviour and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies. This policy is linked, and works alongside the school's Computer Security, Disposal of IT equipment, E-Safety Policy, Safeguarding, Internet Filtering, Anti-Bullying, Behaviour, Communications, Social Media, Handheld Mobile Device & Data Protection policies.
All schools should have an acceptable use policy (AUP). This should detail the ways staff; pupils and all network users (including parents and visitors) can and cannot use ICT facilities.

Responsibility for the appropriate use of ICT

The trust board has responsibility for ensuring that academies have an AUP Policy for ICT and that this policy is reviewed annually.

All staff have a responsibility to use ICT appropriately and legally and report any illegal or inappropriate use of ICT to the Headteacher/CEO or the designated person for E-safety, as soon as possible. All staff should address issues of E-safety when using the internet with children.

Technical staff will ensure that computers have up to date virus protection, the latest security patches installed, and the Academies internet connection is filtered.

Scope of the Policy

This policy applies to all members of the Academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data - see Electronic Devices - Searching & Deletion Policy.

In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place in and out of school.

Roles and responsibilities

Staff:

- All staff have a responsibility to use ICT appropriately and legally and report any illegal or inappropriate use of ICT to the Headteacher/CEO or the designated person for E-safety, as soon as possible.
- All staff should be made aware of this policy

Students / Pupils:

- are responsible for using the academy digital technology systems in accordance with other relevant policies including this policy, e safety and behaviour

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's e-safety Policy covers their actions out of school, if related to their membership of the school
- All pupils must be made aware of this Acceptable user Policy

Parents / Carers:
Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the academy (where this is allowed)

Use of the Internet

The academy encourages users to make effective use of the Internet and such use should always be lawful and appropriate. Internet usage means any connection to the Internet via web browsing.

The school expects all users to use the Internet responsibly and strictly according to the following conditions:

Users shall not:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to: pornography, promote discrimination of any kind**,** promote racial or religious hatred**,** illegal acts any other information which may be offensive to colleagues.
- Engage in incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the police: images of child abuse, adult material that potentially breaches the Obscene Publications Act in the UK**,** criminally racist material in the UK.
- Post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog.
- Engage in on-line gambling or gaming.
- It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

Children that access material that concerns them should follow the information contained in the E-safety Policy.

Managing the Internet

Pupils will have supervised access to Internet resources. Staff will preview any recommended sites before use and raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources. All users must observe copyright of materials from electronic resources.

Internet Filtering

Coast Academies provides an in house filtering service for the internet. The in house system provides a very high level of filtering for staff and pupils with analysis and reporting features. No system is perfect however which is why pupils must be supervised.

See E-safety policy for procedures should any issues be raised.

Data Protection and Computer Security

See Data Protection policy and Data Retention Policy

All users on the system are expected to protect their own login details as a matter of personal and system security. Under no circumstance should people allow other users to have their details or use their login. If at any time a user feels that their password has been seen by another user, they should report this to the Academy Technical staff immediately.

User personal and system security code of conduct:

- Staff should never allow children to logon using the staff members details.
- User logon details should not be shared under any circumstances.
- When entering personal details on a website login you will often be asked if you would like to save your details always say no / deny / Never.
- If accessing school data from home on personal or school provided hardware you should always ensure, by following the aforementioned code that data integrity is respected at all times. Your equipment is more vulnerable once it leaves the building. laptops, mobile technology and pen drives are susceptible to theft and loss along with its data.
- Staff should never use memory sticks in relation to their work
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Computer screens should be locked when absent from PC using Ctrl + Alt + Delete to prevent unauthorised access

Use of data

Staff should never use their position to gain access to information for their own advantage and/or a child's or family's detriment. Also see Staff Code of Conduct Policy

Password Security

Password security is essential for staff, particularly as they can access and use pupil data therefore, staff are expected to have secure passwords which are not shared with anyone. There is a policy in place to force regular password changes.

Staff are provided with individual usernames and passwords to provide access to the school network, email, and Management Information System

Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems, including ensuring that passwords are not shared and are changed (changes are now forced on a regular basis) Individual staff users must also make sure that workstations are not left unattended and are screen locked.

- All users must only use issued passwords to access computer based services.
- Notify the Technical staff if you need to change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- It is suggested that passwords contain a minimum of 8 characters and be difficult to guess.
- Staff and pupils who have left the school will be removed from the system.
- If you think your password may have been compromised or someone else has become aware of your password report this to your Academy Technical staff

Staff Email

Staff are required to read their emails on a daily basis. All email messages sent externally should include a standard disclaimer stating that the content of the email are not necessarily the views of the Academy. Unsolicited email with children is not allowed. Any communication with children via email should be through the staff school email account to the pupil school account only. Do not release or in any way make available personal details of any colleague or pupil (phone numbers or personal e-mail addresses) over the Internet.

Data Transfer

When schools send electronic information about identifiable pupils or staff to each other or to an appropriate outside organisation it MUST be sent by a secure method:

From one school to another or between LA's the s2s (School to School) service should be used.

When staff are required to send pupil/staff data electronically this should be sent using a secure data transfer solution i.e.: RM SecureNet Plus mail, Egress.

Sharing Content

Any content published on the school website/social media is thoroughly checked to ensure that there is no content that compromises the safety of pupils or staff. On entry to the school all parents / carers will be asked to give permission before using images of pupils on the website or other external platforms. We ensure the image file is appropriately named – do not use pupils' full names in image file names or tags if published on the web. If being saved, Images will be appropriately stored and secured on the school's network and deleted in line with our Data retention policy.

Only designated staff have authority to upload to the school website or social media.

Digital Media

Digital media and photographs play an important part of recording events in school life. The academy provides digital cameras, or other devices for use by children and staff.

Pupils are not permitted to use *personal* digital equipment, including mobile phones and cameras, to record images of others, this includes when on field trips.

On entry to school all parents / carers will be asked to give permission about the use of images of their children. For more information please see our GDPR policy

Safe use of images

Taking of images & film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking and sharing of images by staff and pupils

Parents and carers

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school / academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

Storage of images

Images/ films of children are stored on the school's network. Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network unless they have previously, with permission, been shared.

Technical staff have the responsibility of deleting the images when they are no longer required, or the pupil has left the school. This will usually be at the end of each academic school year. Any images kept by staff will be their responsibility and will only be kept with parental consent. Any retained images should not be kept in "one drive" folders or on personal devices.

School laptops & iPads

Staff who are issued with School owned laptops / iPads are required to sign an agreement. Staff must follow the school's guidelines for the laptops / iPad security and maintenance and will be required to return it on a regular basis for updates and audit.

Personal mobile devices for staff

The school allows staff to bring in personal mobile phones and devices for their own use, these must be kept in a secure area and remain on silent throughout teaching time. In the case of wrist devices (such as an Apple Watch) these should be set with notifications off during teaching sessions.

Staff are not usually permitted to use *personal* digital equipment, such as mobile phones, watches and cameras, to record images of pupils. However, with the express permission of the Headteacher or senior staff, images can be taken on personal devices provided they are transferred quickly and deleted from the staff device. There would need to be a clearly understood reason for this use.

Under no circumstances does the school allow a member of staff to contact a pupil or parent / carer using their personal device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.