Student IT and Mobile Device Use Policy

This policy was approved and ratified by Cox Green School

on

6th January 2026

Revision Overview

Version	Area
V2.5	P3, Guidelines, General Conditions, Anti-Virus and Firewall Security, Remote Access, Monitoring and Logging, Severe Breach, Process, Use of Email, Use of the Internet, Monitoring the Use of Email and the Internet, E-Safety Guidelines, Emergent Technologies, Mobile Devices, Appendix 1 (removed)

Key Requirements/Legal Duties

This policy covers the students' use of IT systems and mobile device usage at Cox Green School, including the understanding of e-safety in the use of Internet and email systems. However, the school will also ensure that the government guidance on 'Teaching Online Safety in School' (January 2023) will be adhered to through the curriculum. Students will be taught about how to use technology safely, responsibly, respectfully, and securely within a range of subjects. Topics of internet safety and potential problems online will be covered, with due regard to the school safeguarding policy at all times."

This policy aims to provide students with a clear understanding of the guidelines and consists of four sections:

1. Acceptable use of IT equipment;
2. Use of email and the internet by students;
3. E-Safety including sexting;
4. Use of mobile devices by students.

This policy is linked to our Home School Agreement, the AI Policy and the school's Behaviour for Learning Policy.

The term "students" is used to describe all persons attending the school, in any capacity other than someone covered under the Staff Information Systems and Social Networking Policy; this includes the students enrolled, guest students, and any other person that is not an adult working for the school.

The school does not permit access to the school's corporate network from a personal device; however, it does recognise that students may use a personal device to access school resources in other ways, such as email or remote learning, or via the guest wireless access where preapproved. This policy therefore covers personal devices where used to work on any school work or school services.

As a student of the school, it may not be the device but the user's actions that activate the policy, for example, the use of remote learning from a public computer would still be covered as using school resources remotely are covered in this policy. It is therefore recommended that students read this policy thoroughly.

1. Acceptable Use of IT Equipment

Cox Green School is committed to safeguarding its IT infrastructure to ensure it can be used in the most effective manner to support teaching and learning processes. Ensuring the safety and integrity of the school's ICT infrastructure is the responsibility of all staff and students.

The school encourages students to fully use the IT infrastructure, including portable devices, where no desktop computers are available. The school encourages students to use IT in a responsible way. Portable devices include, for example, laptops and other portable IT devices.

As a user of IT services at the school, you have the right to use its computing services. That right places responsibilities on you as a user, which are outlined below. If you misuse school computing facilities in a way that constitutes a breach or disregard of this policy, consequences associated with that breach will be applied, and you may be in breach of other school policies.

Ignorance of this policy and the responsibilities it places on you is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Students should be advised of this policy during their induction and enrolment at the school, also of the school's requirement for them to adhere to it.

For the purposes of this policy, the term "computing services" refers to any IT resource made available to you, any of the network services, applications or software products that you are provided access to, and the network/data transport infrastructure that you use to access any of the services (including access to the Internet). Students who connect their own IT to the school's guest network and the services available are particularly reminded that such use requires compliance to this policy.

Aims

- To protect the school's networks and equipment;
- To protect the school's data;
- To protect the school, its employees, and its students from activities that might expose them to legal action from other parties or other threats.

Guidelines

Password Security

Access to all systems and services is controlled by a user account and password. Students are allocated their username and password as part of their enrolment with the school. Issuance and continued use of your user account are conditional on your compliance with this policy. Usernames and passwords are not to be shared or revealed to any other party, other than your parent/carer. Those who use another person's user credentials, and those who share such credentials with others, will be in breach of this policy.

The school provides a random password issued to the user on induction, and the user may change this password. Students' passwords must meet the complexity requirements of at least nine characters in length and contain at least four letters of which one must be upper case and three lowercase, two numbers and at least one special character must be used, greater values should be used to improve password security. The first password provided to the user is randomly generated by the school's user account control system, and the user can continue to use this password until prompted to change. Use of strong passwords encourages and supports children's personal cyber security.

It should be noted that the school employs other security measures on top of password complexity to secure student accounts, whilst maintaining proportional levels of access given the age of the users. As such, students cannot access their main user account outside of the UK.

General Conditions

Use of the school "computing services" should be for study and research purposes of the school.

- Your use of the school's computing services must at all times comply with the law.
- Your use of the school's computing services must not interfere with anyone else's use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use (students are prohibited from using any staff devices, including staff laptops).

- You must not access any program or data which has not been specifically authorised for your use, or installed by the school's IT Support.
- You must not use or copy any data or program belonging to another user without their express and specific permission.
- You must not alter the computer material belonging to another user without the user's permission.
- You must not use school computing services to harass, defame, libel, slander, intimidate, impersonate, or otherwise abuse another person or any company or entity.
- You must comply with digital media laws. For example, using an image from the internet without the author's permission is a breach of copyright. Users should only use images marked as "Labelled for reuse" or "Labelled for reuse with modifications" as applicable, or use a website providing images with such license.
- You must not use the school's computing services to conduct any form of commercial activity without the express permission of the Operations Director.
- You must not use the school's computing services to disseminate mass (unsolicited) mailings from a school account or on the school network.
- You must not attempt to install, use, or distribute software on any school device.
- You must not use any peer-to-peer file sharing software on any school device, or personal device on the school network.
- You must not use any IRC (Internet Relay Chat) or messenger software, or other "Messengers", IRC or "chat" clients other than those approved by the school (for example Microsoft Teams).
- You must not post or subscribe to newsgroups, online discussion boards, or email list groups from the school's facilities, unless specifically related to school activities.
- You must not use any form of network monitoring or packet sniffing.
- You must not play computer games of any nature, whether preinstalled with the operating system or available online unless approved by the teacher of the current lesson.
- While in a lesson or in a room allocated for study, you must be working on the set tasks or homework. Students found not to be working on task may be removed from the computer.

Anti-Virus and Firewall Security

All school computers are installed with current versions of virus protection and firewall software by the IT Support department. Users are not to alter the configuration of this software. This software is installed to prevent an attack of malicious software and to prevent loss of data and corruption or encryption of programs/files. Users must ensure that they are running with adequate and up-to-date anti-virus software at all times if they are using a personal device. If any user suspects a viral infection of their device, they should inform the IT Support department immediately. If it is a personal device, the user should disconnect it from the school's guest network immediately. If the IT Support department detects a device behaving abnormally due to a possible viral infection, it will be disconnected from the network until deemed safe.

Physical Security

The users of IT equipment should always adhere to the following guidelines:

- Treat equipment safely, in the same manner as a reasonable person would;

- Keep liquids and food away from the IT equipment;
- Do not place objects on or in IT equipment;
- Any portable device must be returned and put on charge when not in use;
- Report any suspicious behaviour or damage to the class teacher or appropriate member of staff.

Remote Access

All user documents are now stored on Office 365 OneDrive and SharePoint, which allows staff and students to access their documents from various types of devices, along with Office applications in the browser. Most software is now available for students to either access online or install at home for free, please refer to the home learning section of the school website for details.

Monitoring and Logging

Monitoring is carried out in line with UK GDPR and the school's Data Protection Policy, for safeguarding and security purposes. Activities regarding network transactions are monitored, logged, and kept for an appropriate amount of time. Logs are taken for reasons of safeguarding, security, diagnostics, and account/audit reasons. Logs are available only to authorised systems personnel, and are kept for no longer than necessary, in line with current data protection guidelines.

All computer use is recorded and may be monitored. The monitoring system will flag keywords and key activities to the attention of the SAFE team and IT Support team. If the violation is found to be in breach of this or any other school policy, it may be required to pass the information on to the relevant parties. Remote support is also provided using the same system, and access to student computers is available to school staff. All remote-controlled events are logged and accessible to the Operations Director.

Such records and information are sometimes required under law by external agencies and authorities. The school will comply with such requests when formally and correctly submitted. In the event of an internal investigation, logs will be given to the designated investigating officer for review.

Breach of this Policy

Incidents that are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user-related activity for evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy, but in general, such breaches will be categorised into one of three levels of severity, and each level of breach will carry with it a possible range of sanctions, consequences, and/or penalties. In the event equipment is damaged or lost as a result of non-compliance with this policy, or as a result of other negligent action, then you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the school.

The lists below are examples and are not an exhaustive list of breaches for each category.

Minor Breach

This level of breach may attract a verbal warning, which may be held recorded on their student file. In general, this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance. Examples of this level of non-compliance would include:

- Taking food and/or drink into IT facilities where they are forbidden;
- Sending nuisance (non-offensive) email;
- Behaving in a disruptive manner.

Not all first offences will automatically be categorised at this level since some may be of a significance or impact that elevates them to one of the higher levels of severity.

Moderate Breach

This level of breach may attract more substantial sanctions and/or penalties. Examples of this level of non-compliance includes:

- Repeated minor breaches within a 12-month period;
- Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area;
- Assisting or encouraging unauthorised access;
- Misuse of software or software license infringement;
- Copyright infringement;
- Interference with workstation or computer configuration.

Severe Breach

This level of breach may attract more stringent sanctions, penalties, and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded. Damage to equipment could result in a financial contribution being required for a replacement. Examples of this level of breach would include:

- Repeated moderate breaches;
- Theft, vandalism, or wilful damage of/to IT facilities, services, and resources;
- Forging email, i.e. masquerading as another person;
- Using the internet to engage with activities that are a security risk, including risks as identified by the PREVENT agenda;
- Sending abusive, harassing, offensive, or intimidating email;
- Maligning, defaming, slandering, or libelling another person;
- Loading, viewing, storing, or distributing pornographic or other offensive material;
- Unauthorised copying, storage, or distribution of software;
- Any action, whilst using school computing services and facilities, deemed likely to bring the school into disrepute;
- Attempting unauthorised access to a remote system;
- Attempting to jeopardise, damage, circumvent, impair or destroy IT systems security;
- Attempting to modify, damage, or destroy another authorised user's data;
- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing, or network flooding activities;
- Attempting to defraud the school of a school-owned device.

Process

An investigation will be carried out, in confidence, by a member of the SAFE Team under the direction of the Headteacher, with the Operations Director. That investigative report will be passed to the Head of Year to be considered within the academy's disciplinary procedures. Referrals may also be made to the Local Authority and other agencies if an act of terrorism is suspected or safeguarding risks identified.

2. Use of Email and Internet by Students

Principles

The provisions of this policy apply to all students, whether or not they have access to, or sole use of, e-mail/internet on a school or personal computer. Although access to such facilities does not form part of the benefits provided to students, it is recognised that there are occasions when students might legitimately make private use of these facilities. This policy is intended to make clear what constitutes legitimate use. It is intended not to place students under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of e-mail and the Internet.

The sections of the policy covered by behaviour should be read in conjunction with the appropriate student Behaviour for Learning Policy.

Purposes

This policy aims to:

- Provide guidance on inappropriate use of school email, Internet facilities, or school devices;
- Clarify when the school monitors student usage of these facilities and the expectations of students while using these facilities.

Use of Email

- Students may only use school email accounts, on the school systems.
- Students must tell a teacher or their SAFE Manager if they receive offensive emails.
- Students must not reveal details of themselves or others, such as address or telephone numbers, or arrange to meet anyone in email communication.
- Access in school to external personal email accounts is strictly prohibited, and settings to block these are set on the school's filtering system.
- Excessive social email should not be used as it can interfere with learning. Sending and receiving social emails in lessons will be dealt with in the same behavioural framework as other off-task behaviour.
- The forwarding of chain letters is banned.
- Student email accounts may not send bulk emails.
- In the school context, e-mails should not be considered private, and the school reserves the right to monitor the emails of students. The school is mindful of the need to balance the need to maintain the safety of students and the preservation of human rights.
- Email communication between staff and students must, for the protection of both parties, only take place through the school email, where such communication is easily monitored and tracked.
- Private email addresses must not be shared between staff and students.

Use of the Internet

Students will be encouraged to develop skills to allow them to become discriminating and productive Internet users. The skill development opportunities are incorporated into programmes of study in IT and regularly reinforced in other subject areas.

- Internet access will be planned to enrich and extend learning activities.
- Through the curriculum/assemblies and the school website, students will be guided on online activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work.
- The school will encourage practices that ensure that the use of internet-derived materials by students complies with copyright law.
- Students will be taught what is acceptable and what is not acceptable, and given clear objectives for Internet use.
- If students discover unsuitable sites, the URL (website address) and content must be reported to the IT Helpdesk via the class teacher.
- A copy of this policy is available on the Cox Green School website.

The school recognises its responsibilities in protecting students from exposure to unsuitable material. It is impossible, however, whilst maintaining a flexible and responsible system, to remove completely the risk that students might access unsuitable materials.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on the school computers. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- Methods to identify, assess, and minimise risks will be reviewed regularly.
- The school will utilise the filtering systems which have been researched, purchased, and implemented by the school's IT Support department and augment this with other safeguards as appropriate.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the IT Helpdesk.
- Students are informed that Internet use will be monitored by an acceptance form on enrolment, and were able when logging onto school devices, which is referred to in this school policy.
- Misuse of the school's computer system by students will be dealt with in accordance with the school's behaviour policy framework.
- When appropriate, the school's Designated Safeguarding Lead will be involved in accordance with the Child Protection Policy.

Public and unregulated groups, chat rooms, blogs, and online communities can be of educational use, but should be accessed with caution.

- Students will be restricted from access to uncategorised or unproductive public or unregulated chat rooms.
- Students will use only regulated educational chat environments, or as advised by their class teacher. In most circumstances, chat will take place through the school's system.
- The use of the school email is freely accessible around the clock to students.
- Chat and forum communication between staff and students must, for the protection of both parties, only take place through school-approved systems.
- Access to the Internet over the mobile phone network cannot be regulated by the school and is therefore banned for Years 7 to 11, and on all school devices, and must not be used during the school day.

Monitoring the Use of Email and the Internet

The school has systems that monitor all IT facilities, including email, Internet and phone use, and whilst it is within the school's rights to monitor the use of its systems, it does not constantly do so as a matter of routine. However, where there are reasonable grounds to suspect an instance of misuse or abuse of any services provided by the school or on a school device, the school may monitor activities on these services/devices. The school telephone system calls are recorded at all times; details are in the Data Protection policy.

3. E-Safety

Principles

The purpose of this section is to guide students on the safe use of e-resources and the general safe use of the Internet and email. The school uses a web filtering system to reduce the risk of its users entering websites that may pose a risk either to the user, the school's IT infrastructure, or the school's data. When using resources outside of the Cox Green School network, users are not protected by this filtering system and must be aware of the dangers. Many threats exist on the internet, especially on social media sites, and students are likely to be part of multiple social media sites. Information relating to protecting these accounts from such threats by use of privacy settings can be found on most social media sites' help or support pages.

Guidelines

The internet and mobile technology allow ways of communicating quickly and efficiently. However, there are risks and issues attached, particularly when behaviour is neither appropriate nor responsible.

The following rules and guidelines should be noted:

- **Do** inform your parent/carer about any encounters that worry you;
- **Do** set up your privacy settings for any social networking site;
- **Do** ensure your mobile phone/devices are password/PIN protected;
- **Do** share your password/PIN with your parent/carer;
- **Do** allow your parent/carer access to your devices and accounts for your safety;
- **Do** make sure that all publicly available information about you is accurate and appropriate;

- **Do** remember online conversations may be referred to as 'chat', but they are written documents and should always be treated as such;
- **Do** make sure that you know the consequences of the misuse of digital equipment;
- **Do**, if you are unsure who can view online materials, assume that it is publicly available. Remember, once information is online, you have relinquished control of it;
- **Do not** behave in a way that could suggest that you are trying to develop a personal relationship with a member of staff;
- **Do not** give your personal information to strangers. This includes mobile phone numbers, social networking accounts, personal website/blog, online image store sites, passwords etc;
- **Do not** use the Internet or other non-school web-based communication to send personal messages to school staff;
- **Do not** add staff or their relatives as friends or to lists on social networking sites, gaming websites, content-sharing sites, etc. However, sixth formers are permitted to "connect" with staff on LinkedIn, and any other appropriate business-related social media sites on a professional basis to support with professional development.

Threats

The Internet is massive, there are many sites, and the content on them can vary, so you should keep to regular websites where possible and try not to browse unknown websites. There are many malicious websites imitating legitimate ones, such as banking websites. It is recommended that you save legitimate websites to your favourites so you can quickly access them. Many websites have a security certificate, which appears as a padlock in the address bar, and this certificate is a form of certifying the website. It does NOT prove it is a legitimate site, only that the website address you have visited is hosted by the company that owns the domain name.

Some malicious websites contain viruses that can infect your computer just by browsing to the web page, so you should report any suspicious behaviour of your school device to the IT Support team or your teacher. You should ensure you have adequate antivirus protection on your personal device to help protect you from these threats. If you are on a website that does not look/feel right, do NOT proceed.

The school operates a content filtering system and an enterprise-grade firewall. Access to websites is limited, and the ability to access malicious or inappropriate websites is restricted in school. Outside of school, you are likely to be on an unfiltered connection, which allows access to websites that are against school policies (such as Social Networking sites, pornographic sites, hacking sites, etc). To protect yourself against accessing such websites, it is recommended that you check the name of the website before entering it, only enter sites you know, or check the website using a search engine that allows you to obtain a brief summary of the content of the website. Accidental access to inappropriate websites should be reported to your teacher or form tutor, who will notify the IT Support team to note this against the log on the monitoring software.

Other threats include those of other users. Often on legitimate websites, there are users who will attempt to cyberbully, threaten, slander, troll, spam, radicalise etc. It is recommended that you ignore these users or report them to the site's abuse team. Users who are in school should be followed up in line with the school's policies and reported to the SAFE Team, who can take necessary measures.

Accessing account-protected websites on a public computer or public wireless network can expose you to credential theft. Malware or so-called packet sniffing programs can identify login details on unsecure networks. It is recommended that you regularly update your login details and only access secure websites from a secure network connection.

Reporting Abuse

If you receive abuse on school systems of a cyber nature, you should report it to the IT Support team or SAFE team, who can investigate. You should always refer to the school behaviour policies if it is perceived to be coming from another user inside the school.

4. Use of Mobile Devices by Students

Principles

Cox Green School accepts that parents may wish their child to be able to contact them outside of school hours by the use of a mobile phone. The Trustees do not wish to encourage mobile phones on the school site, but endorse the policy for all students as listed below (including Sixth Form).

Emergent Technologies

Senior staff will maintain an up-to-date knowledge of emergent Internet technologies and their potential for delivering educational or institutional benefits. New technologies will only be implemented after a thorough risk assessment carried out by the suggesting member of staff, a Senior Leadership Team member responsible for curriculum IT development, and the Operations Director.

Mobile Devices

Mobile devices will be allowed on the site by students and are subject to the agreed restrictions:

- Phones/devices must be kept in a student's bag and not carried or displayed on a student's person while on the school site during the day;
- They should be turned off at all times unless a member of staff has given a student permission to use their device;
- Students should not use their phones to communicate with parents/other students during the school day;
- Students who bring their mobile devices into school do so at their own risk. The school cannot be held responsible for the safety and security of these devices. The school will not accept any liability for misuse or loss of a mobile phone;
- Students should check with their parents before bringing devices into school, ensuring the device is properly insured and sufficient mobile data is available to avoid additional charges from the mobile service provider;
- Parents should be aware that by providing their child with a mobile device that has a mobile data connection, that this is not filtered and there is access to potentially high-risk sites;
- Any transgression from this policy will result in the mobile phone being confiscated and retained until the end of the school day (See Behaviour Policy). The school reserves the right to vary these arrangements where safeguarding concerns are identified.
- Confiscated mobile device can be collected by the student at the end of the school day at reception.

The school takes incidents of bullying (using mobile phones), sexting, and sharing of nudes and semi-nudes seriously. Such incidents may be referred to the police and the following guidance adhered to:

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

The same policy applies to other portable/mobile devices items such as IPods, MP3 Players, and Smart Watches.

Communication of Policy

This policy will be published on the school website and the staff intranet.

Review of Policy

This is a non-statutory policy and will be reviewed every 3 years, unless there are updates which are required to be made, and will be approved by the Senior Leadership Team.

Version History

Version	Authorisation	Approval Date	Effective Date	Next Review
1	Full Governing Body	July 2013	Sept 2013	July 2015
1.2	Full Governing Body	July 2015	Sept 2015	July 2017
This policy was delegated to the Peoples and External Relations Committee in June 2026				
2	Peoples & External Relations	June 2016	June 2016	June 2019
2.1	Peoples & External Relations	25/11/2016	25/11/2016	June 2019
2.2	Peoples & External Relations	17/01/2017	17/01/2017	January 2020
2.3	Peoples & External Relations	01/10/2019	01/10/2019	October 2022
This policy was delegated to the Cox Green Senior Leadership Team in January 2023				
2.4	Cox Green School Senior Leadership Team	10/01/2023	10/01/2023	January 2026
2.5	Cox Green School Senior Leadership Team	06/01/2026	06/01/2026	July 2026 For changes to mobile devices