eSafety Policy

Reviewed	Date of Next Review	Responsibility
August 2025	August 2026	Principal

Our Mission:

'To enable young people to live and work without barriers'

Our Values:

- **Teamwork –** we hold ourselves and each other to account and are better when we work together
- **Compassion –** we act with trust, honesty, and kindness in everything we do
- **Inclusion –** we treat each other fairly and with respect
- **Innovation –** we encourage thoughtful, creative, and aspirational ideas
- **Pride –** we encourage each other to be proud of who we are and what we do

Contents

This policy applies to all members and sites of the Fairfield Trust (including staff, learners, volunteers, parents and carers, visitors, Trust users) who have access to and are users of College digital systems, both in and out of the College. It also applies to the use of personal digital technology on the College site (where allowed).

Scope of the Online Safety Policy

This eSafety Policy outlines the commitment of Fairfield Trust to safeguard members of our College Trust online in accordance with statutory guidance and best practice. Colleges should be aware of the legislative framework under which this eSafety Policy template and guidance has been produced.

This eSafety Policy applies to all members of the College Trust (including staff, learners, volunteers, parents, carers, visitors, and other Trust users) who have access to and are users of college digital systems, and technologies both in and out of the College. It also applies to the use of personal digital technology on the College site (where allowed).

Fairfield Trust will deal with all incidents identified in this policy (and the College's Safeguarding and Child Protection Policy). For incidents concerning young people, the Trust will, where appropriate, inform parents/carers of incidents of inappropriate online safety behaviour that take place, with an expectation that they will address these concerns and act as we would at Fairfield. Often, issues that arise outside of College can impact on learning, so working together with families to ensure collaborative monitoring of online behaviour across home and school will help keep our learners safe and ensure that issues can be dealt with in a timely manner. Fairfield Trust recognises that it has a duty to support learners and their use of technology on Trust premises and values parents/carers supporting their children to use technology outside of College.

Schedule for Development, Monitoring, and Review

The eSafety Policy has been developed by the Principal and eSafety team and subsequently ratified by Order of the Board. eSafety is overseen and monitored by a group of colleagues (known as the eSafety team) comprising of:

- Principal/DSL
- SLT
- MSA365 Representative
- Nominated Trustee

The eSafety team will monitor the impact of the policy using:

- Staff and learner feedback.
- Logs of reported incidents.
- Monitoring logs of internet activity (including sites visited).
- Internal monitoring data for network activity.
- SchoolPod data including communication with parents.
- Changes to policy and legislation such as the Department for Education (DfE).

Process for Review

Schedule for Monitoring and next Review	Aug 2026 by the Principal
This eSafety Policy was approved by the Trust Board in	April 2024
The implementation of this eSafety Policy will be monitored by	PA to the Trustees & SLT
Monitoring will take place at regular intervals: - Weekly active user blocked searches - Termly online safety group - Annual review of impact	MSA/Principal All Group All Group
The Trust Board will receive a report update around eSafety and all concerns	Annually (at last Education & SG Committee of the year)
The eSafety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place.	

Roles and Responsibilities

Online safety and safeguarding of all colleagues and learners within the Trust is achievable when all members work together. This approach will allow us to develop safe and responsible online behaviours; provide ways to learn from each other and from good practice elsewhere. We can help each other by reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the college.

Principal, Senior Leaders and Safeguarding Team

- currently the Principal is also the DSL, supported by a DDSL, the Safeguarding Team and in addition, a nominated Trustee. Collectively, they monitor and oversee online safety with regular reporting from the Principal to the Trust Board.
- the Principal has a duty of care for ensuring the safety (including online safety) of members of the Trust and fostering a culture of safeguarding, along with the day-to-day responsibility as the DSL and Online Safety Lead.
- the Principal and the nominated Trustee are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (as outlined in the Safeguarding and Child Protection Policy).
- the Principal/senior leaders are responsible for ensuring that Trust staff, external technical staff, and the safeguarding team carry out their responsibilities effectively and receive suitable training to enable them to conduct their roles.
- the Principal and DDSL will ensure that there is a system in place to allow for monitoring and support in carrying out internal online safety monitoring.
- the Trust Board and SLT will receive regular monitoring reports from the Principal.

Designated Safeguarding Lead (DSL)

The DSL will:

- lead the Online Review Group meetings.
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns.
- have a leading role in establishing and reviewing the College eSafety policies/documents.

- liaise with education staff to ensure that the online safety curriculum is planned, mapped, embedded, and evaluated.
- liaise with Trust staff to ensure that they are confident in reporting and monitoring safe use of the technology and the internet.
- monitor and oversee blocked active search reports and follow up where necessary.
- authorise access to search histories where appropriate and ensure that sufficient filtering & monitoring processes are in in place.
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- ensure that staff are familiar with their responsibilities around online safety.
- receive reports of online safety incidents and ensure these are used to inform future online safety developments.
- provide (or identify sources of) training and advice for all members of the Trust.
- liaise with technical staff, pastoral staff, and support staff (as relevant).
- provide reports to the Trust Board to discuss current issues, review (anonymised) incidents (where appropriate) and if possible, filtering and monitoring logs.
- attend relevant Trust Board meetings/groups.
- liaise with the local authority and relevant agencies where needed in the referral and reporting of incidents externally.
- Ensure that there are procedures to restrict:
    - sharing of personal data
    - access to illegal/inappropriate materials
    - inappropriate online contact with adults/strangers
    - potential or actual incidents of grooming
    - online bullying

External IT Provider- MSA365

The IT service provider has technical responsibility for:

- maintaining filtering and monitoring systems.
- providing filtering and monitoring reports.
- completing actions following concerns or checks to systems.
- liaise with the SLT and DSL to:
    - procure systems
    - identify risk
    - carry out reviews
    - carry out checks
- contribute to reviewing filtering and monitoring arrangements.
- updating the Trust on best practice, legislative updates around IT procurement and practice.
- ensuring that we are compliant under the filtering and monitoring expectations set out by the Government for education.

Trustees

Trustees are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy at least annually. The reviewing of the impact and effectiveness of the policy will take place with the Principal, MSA365 and the nominated Trustee.

Education Staff (Tutors, LSA, JCs and WBL leads)

Education Staff will work with the DSL and the Education Manager to develop a planned and coordinated online safety education programme. This will be delivered through:

- a discrete programme of specific interventions for young people
- the Personal Growth and Wellbeing Programme
- rolling CEOP Training for the education team
- tutorial focus at key points in the year
- through relevant national initiatives and opportunities

All staff are responsible for ensuring that:

- they understand the Trust's eSafety Policy and practices.
- they understand that online safety is a core part of safeguarding.
- they have read, understood, and signed the staff acceptable use agreement (AUA).
- They must immediately report any suspected staff or concerns through SchoolPod, in line with the College safeguarding procedures.
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official College systems.
- online safety issues are embedded in all aspects of the curriculum and referred to in real-time as part of learning.
- ensure learners understand and follow the e Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they support the College's agreement on not using personal digital technologies, mobile devices in lessons and other College activities.
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of College and in their use of social media. Use of social media guidance can be found in the staff handbook.
- They support young people to report concerns through the online reporting tool.

Onsite IT Engineer

Is responsible for ensuring that:

- they are aware of and follow the College eSafety Policy and carry out their work effectively in line with College policy.
- the College technical infrastructure is secure and is not open to misuse or malicious attack.
- the College meets (as a minimum) the required online safety technical requirements as identified by relevant bodies (such as KCSIE, Filtering and Monitoring standards).
- there is clear, safe, and managed control of user access to networks and devices with the adequate permissions and decisions logged in all instances.
- staff are required to sign a mobile device agreement outlining their responsibilities for all hardware supplied by the Trust.
- they respond quickly and effectively to all requests made by the Online Safety Group, Senior Leaders, DSL/DDSL with regard to student safety.
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Principal for investigation and action.
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring software/systems are implemented and regularly updated as agreed in College policies.

Learners

- are responsible for using the College digital technology systems in accordance with the Learner Acceptable Use Agreement.
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of College and realise that the College's eSafety Policy covers their actions out of College, if related to their membership of the College.

Parents and Carers

The College will take every opportunity to help parents and carers understand these issues through:

- publishing the College Online Safety Policy on the College website.
- providing them with a copy of the learners' acceptable use agreement as part of induction.
- publish information about appropriate use of social media, relating to posts concerning the College.
- seek explicit consent for media use, images, and online information both for internal and external College use.
- provide a dedicated page on the website for parents and carers.

Parents and carers will be encouraged to support the College in:

- reinforcing the online safety messages provided to learners in College.
- taking full responsibility for giving their child a personal device and supporting young people to understand the difference between personal and public use of technology.

Trust Staff

Trust staff who access College software will be expected to sign a Trust User AUA before being provided with access. The Staff Handbook also contains social media guidance re the expectations around how staff use social media and technology both in and outside of College. It is recognised that regardless of role, location or site, the safety of our young people and colleagues is paramount.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the College Trust, with responsibility for issues regarding online safety and monitoring the eSafety Policy including the impact of initiatives.

The Online Safety Group has the following members:

- Nominated Trustee
- Designated Safeguarding Lead
- Senior Leaders
- MSA365 Engineer
- Representation from Education, Commercial and YPS

Members of the Online Safety Group will assist the DSL/Principal with:

- the production/review/monitoring of the College eSafety Policy/documents.
- the review of the College filtering policy.
- mapping and reviewing the impact of online education/curriculum.
- encouraging the contribution of learners to staff awareness, emerging trends, and the College online safety provision.
- consulting stakeholders – including staff/parents/carers about the online safety provision.

POLICY

eSafety Policy

The College eSafety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- allocates responsibilities for the delivery of the policy.
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the College and how they should use this understanding to help safeguard learners in the digital world.
- describes how the College will help prepare learners to be safe and responsible users of online technologies.
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- is supplemented by a series of related acceptable use agreements.
- is made available to staff at induction and through PeopleHR and the Staff Handbook.
- is published on the College website.

Acceptable Use

The College has defined what it regards as acceptable/unacceptable use, and this is shown in the tables below:

An Acceptable Use Agreement is a document that outlines a College's expectations on the responsible use of technology by its users which is signed by staff and students that use technology provided by the Trust to demonstrate agreement.

Acceptable use agreements:

The Online Safety Policy and acceptable use agreements define acceptable use at the College. The acceptable use agreements will be communicated/re-enforced through:

- induction and tutorial
- staff induction and handbook
- digital signage
- device agreements
- adherence to policy and practice
- training and updates - such as Cyber security, online safety and KCSIE
- posters/notice displayed
- communication with parents/carers
- built into education sessions
- college website
- peer support

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals, or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e. revenge and extreme pornography. • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					**X**
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to College networks, data, and files, through the use of computers/devices • Creating and propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer /network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					**X**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
In instances of the user actions below, the Principal and SLT will decide whether these should be dealt with internally or by the police. Serious or repeat offences will be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information **here**						
Users shall not undertake activities that are not illegal but are classed as unacceptable in College policies:	Accessing inappropriate material/activities online in a college setting including pornography, gambling, drugs*				X	
	Promotion of any kind of discrimination				X	
	Using systems to run a private business				X	
	Using systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the College				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X**	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the college or brings the College into disrepute				X	

* The IT Provider will perform regular testing of filters, penetration testing and blocked content. This will be recorded through the Smoothwall reporting system and is tested through a specific test account for this purpose only.

** The IT Provider may need to download executable, or large files as part of the maintenance and provision of IT services.

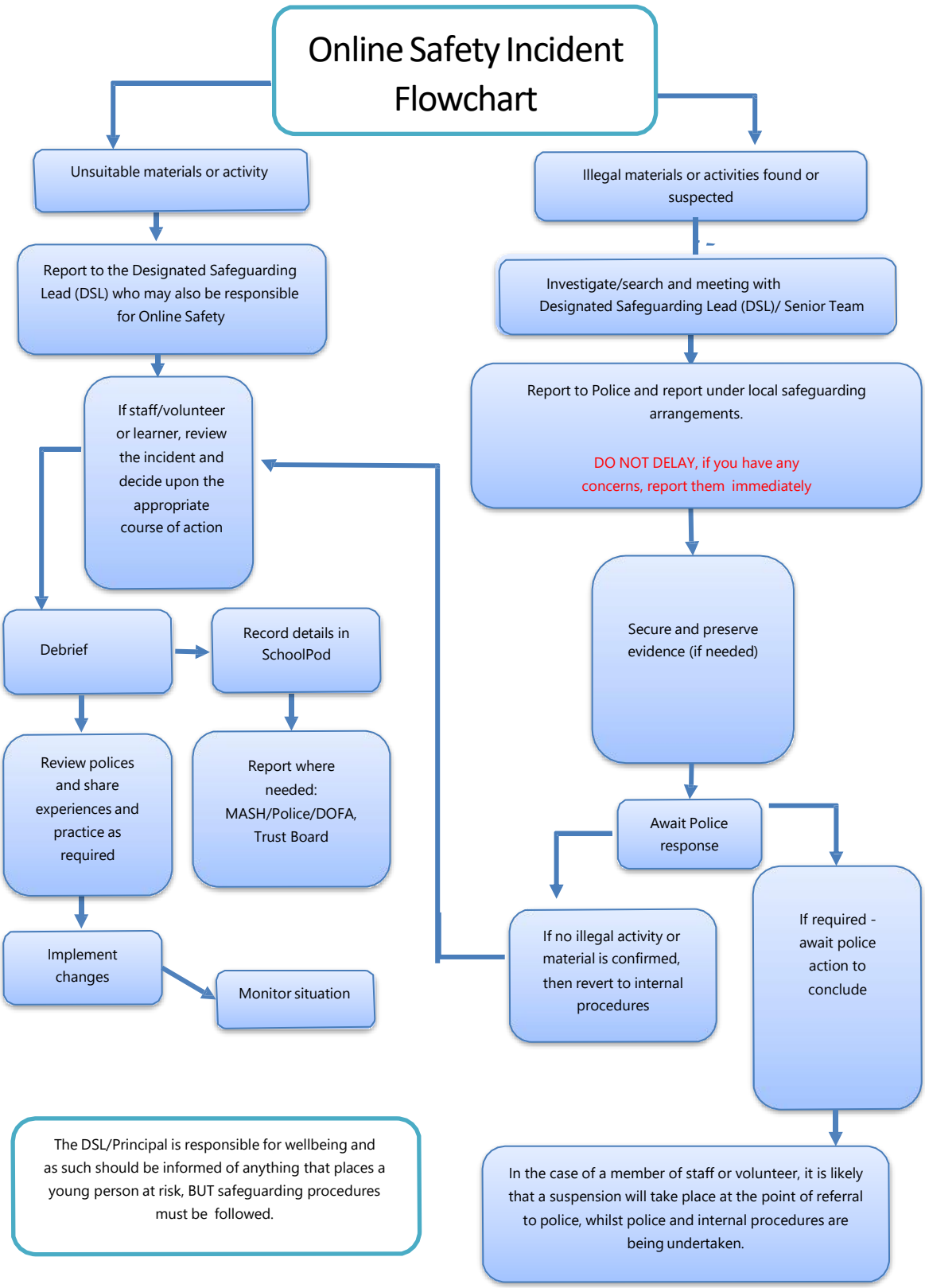
Using Trust Devices	STAFF (inc. volunteer)				LEARNERS (trainee, STEPS, YPS, learner)			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	X				X			
Online shopping/commerce as part of T&L		X				X		
File sharing (between staff/sites/professionally)		X					X	X
Accessing personal social media	X				X			
Messaging/chat through College software		X				X		
Entertainment streaming e.g. Netflix, Disney+			X	X			X	X
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			X	X			X	X
Use of Trust mobile technologies for learning at College		X				X		
Personal use of mobile technologies whilst working	X				X			
Taking photos on Trust mobile devices with relevant consent.		X				X		
Use of other personal devices, e.g. tablets, gaming devices	X				X			
Use of personal e-mail for Trust business.	X				X			
Use of College e-mail for personal e-mails	X				X			

Reporting and Responding

The College will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of the College (with impact on the College) which will need intervention. The College will ensure:

- there are clear reporting routes which are understood and followed by all members of the Trust which are consistent with the College safeguarding procedures, and with the whistleblowing and complaints policies.
- all members of the College Trust will be made aware of the need to report online safety issues/incidents.
- reports will be dealt with as soon as is practically possible once they are received.
- the DSL, and Safeguarding Team have appropriate skills and training to deal with online safety risks and are aware of external sources of support and guidance in dealing with online safety issues, eg local authority; police; Reporting and CEOP.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed College safeguarding procedures.
- any concern about staff misuse will be reported to the Principal, unless the concern involves the Principal, in which case the complaint is referred to the CEO.
- All people involved with any investigation can expect feedback about the outcome and any follow up action.

Below, is a flowchart that outlines the process any online safety incident will follow.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action
Debrief
Record details in SchoolPod
Review polices and share experiences and practice as required
Report where needed: MASH/Police/DOFA, Trust Board
Implement changes
Monitor situation
The DSL/Principal is responsible for wellbeing and as such should be informed of anything that places a young person at risk, BUT safeguarding procedures must be followed.
Illegal materials or activities found or suspected
Investigate/search and meeting with Designated Safeguarding Lead (DSL)/ Senior Team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately
Secure and preserve evidence (if needed)
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures
If required - await police action to conclude
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

College Actions

It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Trust are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows. The following chart is indicative rather than exhaustive, and each case will be dealt with on its individual context.

Responding to Learner Actions

Incidents	Refer to tutor	Refer to Principal	Refer to Police	Report to MSA365	Inform parents/ carers	Remove device/ rights
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X			
Attempting to access or accessing the College network, using another user's account (staff or learner), or allowing others to access college network by sharing username and passwords.	X					
Corrupting or destroying the data of other users.	X			X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.	X	X			X	X
Unauthorised downloading or uploading of files or use of file sharing.	X	X		X	X	X
Using proxy sites or other means to subvert the College's filtering system.	X	X		X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X		X	X	
Deliberately accessing or trying to access offensive or pornographic material.	X	X		X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X		X		
Unauthorised use of digital devices (including taking images).	X			X		
Unauthorised use of online services.	X	X		X		
Actions which could bring the College into disrepute or breach the integrity or the ethos of the College.	X	X			X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X		X	X	X

Responding to Staff Actions

	Refer to Line Manager	Refer to Principal	Refer to HR	Refer to Police	Refer to LA/DoFA	Refer to MSA365
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	
Deliberate actions to breach data protection or network security rules.	X	X	X			X
Deliberately accessing or trying to access illegal, offensive, or pornographic material.	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.	X	X	X			X
Using proxy sites or other means to subvert the College's filtering system.	X	X	X			X
Unauthorised Breaching copyright or licensing regulations.	X	X	X			X
Allowing others to access the College network by sharing username and passwords or attempting to access or accessing the college network, using another person's account.	X					X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.	X		X			X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers.	X	X	X		X	X
Inappropriate personal use of the digital technologies e.g. social media/personal e-mail.	X	X	X			X
Actions which have the potential to bring the College into disrepute or breach the integrity or values of the College.	X	X	X			X
Careless use of personal data, e.g. displaying, holding, or transferring data in an insecure manner.	X	X	X			X
Actions which could compromise a staff member's professional standing.	X	X	X			

Training and Education

Learners

- the Personal Growth and Wellbeing Programme focuses on healthy relationships, including online and also awareness of safety and resilience.
- Tutorial provides a space for exploration and discussion.
- real time interventions support understanding and development.
- a specialist colleague trained in CEOP is delivering targeted sessions to groups of learners that have been identified as needing additional support.
- national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying Week are used to support and develop understanding.
- learning activities are matched to need; are age-related and build on prior learning.
- learners are helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside College.

Staff/Volunteers

All new staff will receive

- induction outlines training, Recording & Reporting, software, expectations etc.
- IT Agreement signed by all employees.
- policies are signed (eSafety & Online protection).
- mobile Device Agreement outlines expectations.
- Cyber Security, Prevent and online protection training updates where appropriate.
- KCSIE updates annually.
- Staff Handbook (signed) outlines expectations and Social Media guidance.

The Designated Safeguarding Lead will have in addition:

- DSL Advanced Safeguarding Training.
- Prevent Referrals Training – GCHQ.
- Senior Mental Health Lead.
- Annual Advanced Certificate in Online Safety for DSLs.
- Cyber Security and PREVENT Training.

Trustees

Trustees will take part in online safety training/awareness sessions, with particular importance for those who are members of the Young People & Safeguarding Committee and those with specific roles for Safeguarding as named in our Safeguarding Policy. See below:

- attendance at training and professional updating through the SWALSS & NATSPEC Safeguarding Network.
- participation in College training and updates.
- advanced Safeguarding training will be undertaken by the Trustee with responsibility for Safeguarding as named in the Trust's policy.

Technology, Filtering and Monitoring

The Trust is responsible for ensuring that the College infrastructure/network is as safe and secure as is reasonably possible and that the procedures approved within this policy are implemented. The College should ensure that all staff are made aware of policies and procedures in place on a regular basis and it is explained that everyone is responsible for online safety and data protection. All Trust polices are reviewed regularly and updates circulated through PeopleHR for all staff to read and sign.

Filtering

- the College undertakes an annual audit of its filtering and monitoring processes to ensure that they are effective.
- the College filters and monitors all user accounts, regardless of the device or role within the Trust.
- Smoothwall, Barracuda and BitDefender are used across the Trust.
- the College manages access to content across its systems for all users. The filtering and monitoring is audited using the guidance set out by regulators. The current audit is available on request.
- access to online content and services is managed for all users.
- illegal content (eg child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content.
- there are differentiated user-level filtering and account permissions depending on age, phase, and role.
- all change-requests are tracked that demonstrate action taken and decision making.
- filtering logs are regularly reviewed and alert the DSL to breaches of the filtering policy, which are then acted upon.

Monitoring

The College has monitoring systems in place to protect the College, systems, and users:

- the College (delegated to MSA365) monitors all network use across all its devices and services.
- real-time schedule reporting is in place for all users.
- real-time notification is in place for attempts at accessing inappropriate content allowing for rapid safeguarding intervention through real time notification in SchoolPod.
- active user breaches of filtering are recorded, and all staff understand this and have agreed to adhere to safer working practices.
- the DSL and MSA365 collectively are responsible for managing the monitoring processes.
- harmful content reporting tools are pushed out to all devices on log in. They can be accessed through the online link which is set as a pop up.
- management of serious safeguarding alerts will be through the Safeguarding policy and practice.
- technical monitoring systems are up to date and managed and logs/alerts are kept for audit purposes.

The College follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and College systems through the use of the appropriate blend of strategies including:

- physical monitoring (adult supervision in the classroom).
- internet use is logged, regularly monitored, and reviewed.
- filtering logs are regularly analysed, and breaches are reported to senior leaders.
- pro-active alerts inform the College of breaches to the filtering policy, allowing effective intervention.

Technical Security

The College technical systems managed by MSA365 ensures:

- that the College's systems and processes are audited.
- Trust systems and security (such as penetration testing or filtering testing through SWGfL) are tested periodically with the results recorded.
- servers, wireless systems, and cabling are securely located and physical access restricted.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- all users have clearly defined access rights to College technical systems and devices. Details of the access rights available to groups of users will be recorded by MSA365.
- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security.
- all College networks and systems will be protected by secure passwords. Passwords must not be shared with anyone.
- the master account passwords for the College systems are kept in a secure place.
- MSA365 is responsible for ensuring that all software purchased by and used by the College is adequately licenced and that the latest software updates (patches) are licenced as necessary.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, and devices from accidental or malicious attempts which might threaten the security of the College systems and data. These are tested regularly. The College infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.

Mobile Technologies

Mobile technology devices issued by the Trust fall under the remit of this policy. For the purposes of practice or expectation, all reference to eSafety, or technology throughout this policy cover all forms of hardware whether desk based, portable or wearable. Staff are not permitted to wear technology at work that has the capacity to record (audio/visual) whilst they are engaged in any intimate or personal care situation. Under no circumstances are staff to use their personal devices for College or Trust related business.
It is the Trust's responsibility to provide adequate technology for staff to fulfil their contractual obligation.

All hardware owned by the Trust is covered by the Policy regardless of site, role, or function. Each device will be accompanied with a Mobile Device Agreement (MDA) that sets out additional responsibilities including liability for acceptable use. All users will sign an MDA and AUP before technology is issued.

All mobile devices are subject to the same level of monitoring and filtering and for the purposes of consistency, are not distinguishable from that which is covered herein.

For further information on using personal devices and Social Media use, please refer to the Staff Handbook.

APPROVED BY THE BOARD OF TRUSTEES

Dr Graeme Athey
Principal

August 2025