Aspiration & Achievement | Resilience & Responsibility | Courage & Confidence

eotas|swindon

better choices for better lives

47. E-Safety Policy

Date adopted: October 2024
Next review: September 2025

See EOTAS policy control document (held by the Business Manager) for status, notes and actionsabout this policy

Aspiration & Achievement | Resilience & Responsibility | Courage & Confidence

E-Safety Policy

Version	Status	Date	Title of Reviewer	Purpose/Outcome
1.0	adopted	September 2024	Headteacher	Adoption of E-safety policy

Contents

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Management Committee on	
The implementation of this Online Safety policy will be monitored by the:	Designated Safeguarding Lead, GDPR Compliance Officer and Business Support Manager
Monitoring will take place at regular intervals:	Termly and immediately in the instance of a breach in policy
The Management Committee will receive a report on the implementation of the Online Safety Policy generated by the Designated Safeguarding Lead/Deputy Designated Safeguarding Lead Team (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online Safety Policy will be reviewed annually or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2025
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding Officer, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity (Securus)
- Surveys/questionnaires of
    - students/pupils
    - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, and community users) who have access to and use EOTAS Swindon digital technology systems, both inside and outside EOTAS Swindon.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable to regulate the behaviour of students/pupils when they are off the school site and empowers staff members to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other Online Safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school. The 2011 Education Act increased these powers concerning the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

EOTAS Management Committee

The EOTAS management committee is responsible for approving the Online Safety Policy and reviewing its effectiveness. The Designated Governor for Safeguarding will also monitor online safety as part of the

annual Safeguarding Audit.

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our school community, it is important that all members of that community work together to develop safe and responsible online behaviours, learn from each other and good practices elsewhere, report 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 school.

Headteachers and senior leaders

- The headteacher has a duty of care to ensure the safety (including online safety) of members of the school community and fostering a culture of safeguarding. However, the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another senior leadership team member should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a staff member·
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to monitor and support those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Designated Safeguarding Lead - Online Safety Officer

Keeping Children Safe in Education states that:
"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."
They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"

*They (the DSL) "*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

While the DSL is responsible for online safety and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to support the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen

The DSL will:

- hold the lead responsibility for online safety within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the

risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensure that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents, handling them, and deciding whether to make a referral by liaising with relevant agencies and ensuring that all incidents are recorded.
- Liaise with staff and IT providers on matters of safety, safeguarding, and welfare (including online and digital safety).

Online Safety Lead

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL) (where these roles are not combined)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school's online safety policies/documents
- promote awareness of and commitment to online safety education/awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- 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 report those incidents immediately
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with technical staff, pastoral staff and support staff
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) concerning the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education program
This will be provided through:
- PHSE and SRE programs
- A mapped cross-curricular program
- assemblies and pastoral programs
- online safety program
- through relevant national initiatives and opportunities e.g. *Safer Internet Day* and *Anti-bullying week*.

Network Manager / Technical staff

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

The contracted IT support team from St Joseph's College ensure

- that the EOTAS Swindon's technical infrastructure is secure and is not open to misuse or malicious attack
- that the EOTAS Swindon meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network internet, remote access, and email is regularly monitored so that any misuse / attempted misuse can be reported to the Headteacher / Designated Safeguarding Lead
- that monitoring software/systems are implemented and updated as agreed in EOTAS Swindon policies

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety 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 immediately report any suspected misuse or problem for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and *parents/carers are on a professional level and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned, learners are 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*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online bullying, sexual harassment, discrimination, hatred, etc
- They model safe, responsible, and professional online behaviours through their own use of technology, including out-of-school and social media.

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Students / Pupils:

- are responsible for using the EOTAS Swindon digital technology systems following the Student/Pupil Acceptable Use Agreement
- 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 using mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and online bullying.
- should understand the importance of adopting good online safety practices when using digital technologies out of school and realise that the EOTAS Swindon Online Safety Policy covers their actions out of school if related to their membership of the school

Parents / Carers

Parents and carers play a crucial role in ensuring their children understand the need to appropriately use online services and devices.

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

- publishing the school's Online Safety Policy on the school website
- Provide them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant websites/publications, e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Community users

Community users who access school systems, websites, or learning platforms as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

The school encourages the engagement of agencies/members of the community who can make valuable contributions to online safety and actively seeks to share its knowledge and good practices with other schools and the community.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the EOTAS Swindon Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Designated Safeguarding Lead will receive regular updates by attending external training events (e.g., from SWGfL / LA / other relevant organisations) and reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings / INSET days.
- The Designated Safeguarding Lead will provide advice/guidance/training to individuals as required.

Training – Governors / Directors

Governors / Directors should take part in online safety training/awareness sessions, with particular importance for the Governor for Safeguarding

Technical – infrastructure/equipment, filtering and monitoring

The EOTAS Swindon will ensure that the EOTAS Swindon infrastructure/network is as safe and secure as reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will effectively carry out their online safety responsibilities. This will be managed by a contract and service level agreement with St Joseph's College.

- EOTAS Swindon technical systems will be managed in ways that ensure that the EOTAS Swindon meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of EOTAS Swindon technical systems
- Servers, wireless systems, and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to EOTAS Swindon technical systems and devices.
- All users will be provided with a username and secure password by the St Joseph's College IT team, who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password
- The "master/administrator" passwords for the EOTAS Swindon ICT systems, used by the Network Manager (or another person), must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place (eg EOTAS Swindon safe)
- EOTAS Swindon Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored
- There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist

material when accessing the internet.

- EOTAS Swindon has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)
- EOTAS Swindon technical staff regularly monitor and record users' activity on the school technical systems, and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc., from accidental or malicious attempts that might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.
- Personal use of EOTAS mobile devices such as phones and laptops is not permitted
- Staff should not download programmes or install executable files on EOTAS devices
- Where possible, staff should access the terminal server remotely or use the Business 365 Portal provided by EOTAS Swindon to access data and information remotely. Memory sticks, DVDs, CDs and other removable media can only be used if properly encrypted
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured
- The school's Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies

School owned/provided devices:

- Will be allocated by Heads of Centre/Business Manager
- Are available for use in and out of school
- Are not available for personal use
- Management of devices/installation of apps / changing of settings/monitoring will be the responsibility of the technical team, and modifications should not be made other than by this team
- Technical support will be offered via the helpdesk at helpdesk@stjosephscollege.net
- Users may only use the cloud services provided by EOTAS
- All users of EOTAS mobile devices will be GDPR trained and will ensure personal data is kept secure
- Images should only be taken for the recording of progress or achievement. Any images of pupils must only be taken if we have a prior written agreement from parents or carers
- EOTAS devices will be returned to the Head of Centre or delegated representative before the employee leaving the EOTAS service
- Deliberate damage or negligent loss will be the responsibility of the employee. Other liabilities will be the responsibility of EOTAS Swindon
- Staff training will be provided via EOTAS Swindon

Personal devices:

- Staff and visitors are allowed to use personal mobile devices in school. Students are not allowed to use personal devices
- Staff may use personal devices for EOTAS business provided the device is password protected, and no student or parent data is stored on the device
- Personal devices should not be connected to the school’s wireless internet other than through remote access to the terminal server
- Technical support is not available for personal mobile devices
- Data Protection regulations apply to any device used to access school systems remotely. Failure to take adequate precautions to secure the personal data of pupils or colleagues may result in disciplinary action
- Personal mobile devices should not be used to take images of pupils

- EOTAS Swindon is not responsible for any loss/damage or malfunction of a personal mobile device following access to the network
- The safe and responsible use of mobile devices is included in the school's Online Safety education programmes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks of publishing digital images online. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication, and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the Internet, e.g., on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website / social media / local press
- Following guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at EOTAS Swindon events for their own personal use (as the Data Protection Act does not cover such use). 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.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but they must follow EOTAS Swindon policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on EOTAS Swindon equipment; staff personal equipment should not be used for such purposes.
- Care should be taken when taking digital / video images to ensure that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or EOTAS Swindon into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on using such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's / Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has an effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where,

why and which member of staff has responsibility for managing it

- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly *what personal data is held*, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes for which it was collected. The school's retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- has procedures in place to deal with the individual rights of the data subject,
- carries out Data Protection Impact Assessments (DPIA) where necessary, e.g. to ensure the protection of personal data when accessed using any remote access solutions or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection-compliant contracts in place with any data processors
- Understand how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- *reports any relevant breaches to the Information Commissioner* within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. To do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- Provide data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- The device will be password protected.
- the device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below), once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times, take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request, whether verbal or written, and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices.
- use personal data only on secure password-protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data
- Transfer data using encryption, a secure email account (where appropriate), and secure password-protected devices.

Communications

	Staff					Pupils			
Communication technologies	Allowed	Allowed at certain times	Allowed for selected staff	Should be avoided	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the EOTAS Swindon	X								X
Use of mobile phones in lessons				x					x
Use of mobile phones in social time				x					x
Taking photos on mobile phones / cameras		x							x
Use of other mobile devices e.g. tablets, gaming devices		x							x
Use of personal email addresses in EOTAS Swindon , or on EOTAS Swindon network				x					x
Use of EOTAS Swindon email for personal emails				x				x	
Use of messaging apps		x							x
Use of social media		x							x
Use of blogs		x							x

When using communication technologies the EOTAS Swindon considers the following as good practice:

- The official EOTAS Swindon email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the EOTAS Swindon email service to communicate with others when in school, or on EOTAS Swindon systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the EOTAS Swindon policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) EOTAS Swindon systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the EOTAS Swindon website and only official email addresses should be used to identify members of staff.

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or school staff.
- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- Each school should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- 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 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 learners in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.
-

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through

- Public-facing website
- Social media
- Online newsletters

The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.
Where learner work, images or videos are published, their identities are protected, and full names are not published.
The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from EOTAS Swindon and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school, either because of the age of the users or the nature of those activities.
The EOTAS Swindon believes that the activities referred to in the following section would be inappropriate in a EOTAS Swindon context and that users, as defined below, should not engage in these

activities in / or outside the EOTAS Swindon when using EOTAS Swindon equipment or systems. The EOTAS Swindon policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the EOTAS Swindon					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use					X	

Aspiration & Achievement	Resilience & Responsibility	Courage & Confidence				
of the internet)						
On-line gaming (educational)			X			
On-line gaming (non-educational)			X			
On-line gambling					X	
On-line shopping / commerce				X		
File sharing		X				
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. Youtube		X				

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:
"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:

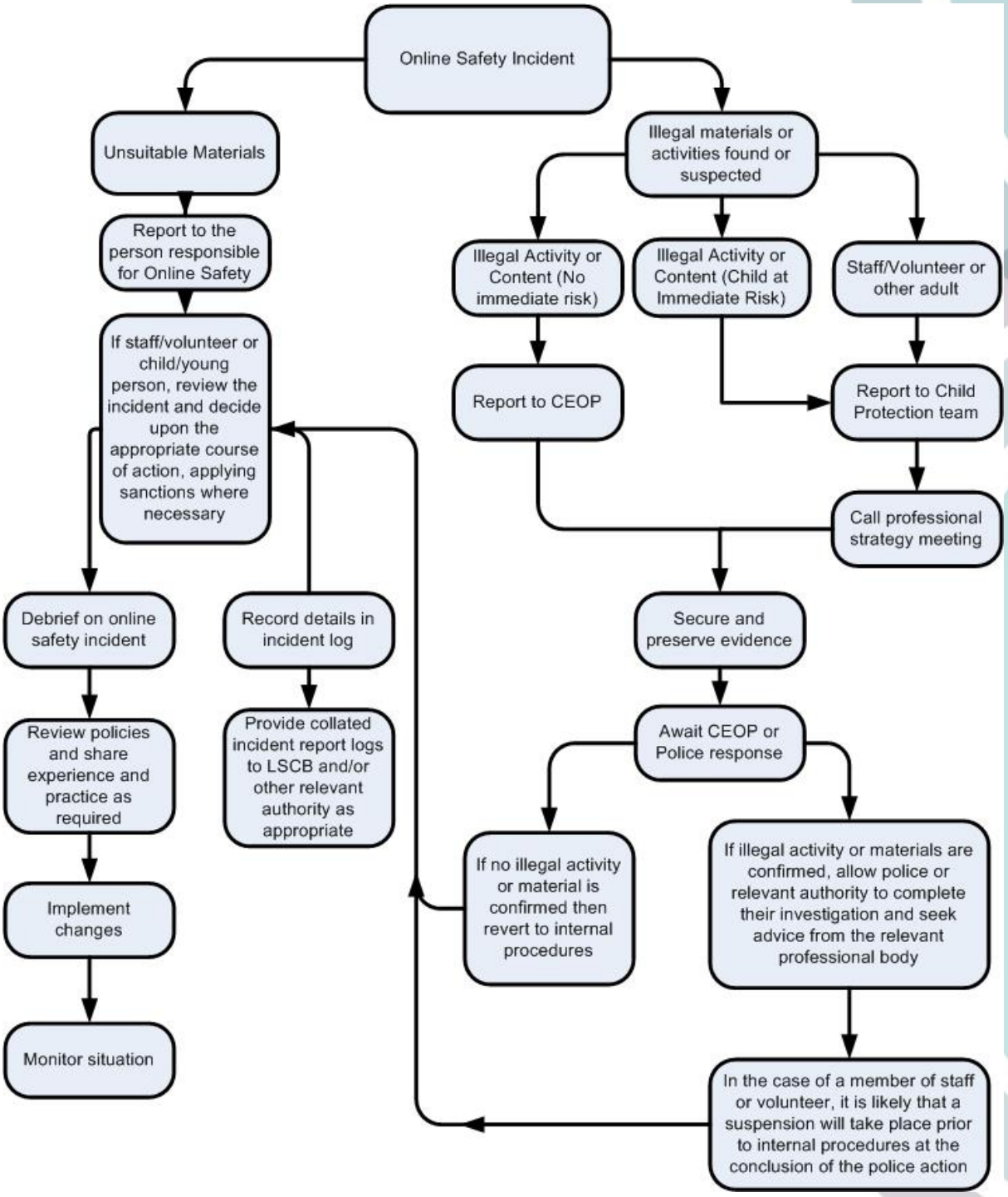
- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

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

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community 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 Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- 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 school safeguarding procedures, this may include
    - Self-generated images
    - Non-consensual images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography

        - Sale of illegal materials/substances
        - Cyber or hacking offences under the Computer Misuse Act
        - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Director of Education
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged via CPOMs
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police;
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to:
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
- governors, through regular safeguarding updates
- local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



Other Incidents

It is hoped that all members of the EOTAS Swindon community will be responsible users of digital technologies, who understand and follow EOTAS Swindon policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the EOTAS Swindon and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

EOTAS Swindon Actions & Sanctions

It is more likely that the EOTAS Swindon 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 school community 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. Incidents will be investigated and some but not necessarily all of the actions will be applied.

Actions / Sanctions

Aspiration & Achievement	Resilience & Responsibility				Courage & Confidence				
Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year /	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X					
Unauthorised use of non-educational sites during lessons	X								
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X								
Unauthorised / inappropriate use of social media / messaging apps / personal email	X								
Unauthorised downloading or uploading of files	X								
Allowing others to access EOTAS Swindon network by sharing username and passwords	X							X	
Attempting to access or accessing the EOTAS Swindon network, using another student's / pupil's account	X							X	
Attempting to access or accessing the EOTAS Swindon network, using the account of a member of staff	X							X	
Corrupting or destroying the data of other users	X					X		X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X					X		X	
Continued infringements of the above, following previous warnings or sanctions						X	X		X
Actions which could bring the EOTAS Swindon into disrepute or breach the integrity of the ethos of the school						X	X	X	X
Using proxy sites or other means to subvert the						X	X		

Aspiration & Achievement	Resilience & Responsibility					Courage & Confidence				
EOTAS Swindon's filtering system										
Accidentally accessing offensive or pornographic material and failing to report the incident	X							X		
Deliberately accessing or trying to access offensive or pornographic material						X	X	X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act								X		

Staff Incidents	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X							
Unauthorised downloading or uploading of files	X							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X							
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X						X
Deliberate actions to breach data protection or network security rules	X	X						X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X				X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X						X
Actions which could compromise the staff member's professional standing	X	X				X		X
Actions which could bring the EOTAS Swindon into disrepute or breach the integrity of the ethos of the EOTAS Swindon	X	X				X		X
Using proxy sites or other means to subvert the EOTAS Swindon's filtering system	X	X				X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material		X					X	X
Breaching copyright or licensing regulations	X					X		
Continued infringements of the above, following previous warnings or sanctions	X	X						X

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Acknowledgements

This policy is based on the SWGFL policy template for schools. SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids