

CROSFIELDS SCHOOL

Online Safety Policy

Policy Owner:	Director of Digital Strategy
Reviewed on:	September 2025
Next Review due:	September 2026
Approved By:	Head & Safeguarding Governor

Contents

Scope of the Online Safety Policy.....	2
Schedule for development, monitoring and review	3
Process for monitoring the impact of the Online Safety Policy	3
Policy and leadership.....	4
Responsibilities.....	4
Online Safety Group.....	8
Online Safety Policy	9
Acceptable use	10
User actions	10
Reporting and responding.....	12
Online Safety Incident Flowchart.....	15
Online Safety Education Programme	16
Contribution of Pupils.....	17
Staff/volunteers	17
Governors.....	17
Families.....	18
Technology	18
Filtering & Monitoring.....	18
Filtering.....	19
Monitoring	19
Mobile technologies.....	21
Social media	21
Digital and video images	22
Online Publishing.....	23
Data Protection	24

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Crosfields School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, Pupils, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Crosfields School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the <i>school governing body</i> on:	September 2025
The implementation of this Online Safety Policy will be monitored by:	Siobhan McClure
Monitoring will take place at regular intervals:	Annually
The <i>governing body</i> will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Termly
The Online Safety 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. The next anticipated review date will be:	September 2026
Should serious online safety incidents take place, normal safeguarding procedures should be followed as per the schools safeguarding policy. This may entail reporting incidents to the Police, CEOP or Children's Services.	As appropriate

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using reported incidents and Filtering and monitoring logs.

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, learning from each other and from good practice elsewhere, 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 school.

Head and SLT

- The Head has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The Head and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head is responsible for ensuring that the Designated Safeguarding Lead / Director of Digital Strategy 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 Head/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Head/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Director of Digital Strategy.
- The Head/senior leaders will work with the responsible Governor, the Designated Safeguarding Lead and European Electronic (EE) in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This responsibility is delegated to Mark Turner as the Safeguarding Governor.

This review will be carried out by the Safeguarding and Welfare Committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Director of Digital Strategy
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to the Safeguarding and Welfare Committee
- membership of the school Online Safety Group

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

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 ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to the Head/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, ensuring that all incidents are recorded.
- liaise with staff and the IT services team on matters of online and digital safety

Director of Digital Strategy

The Director of Digital Strategy will:

- lead the Online Safety Group

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- 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 online safety policies/documents
- promote an 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 immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/pupils
- liaise with school technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined In Keeping Children Safe in Education:
 - content
 - contact
 - conduct
 - commerce

Curriculum Leads

Curriculum Leads will work with the DSL/Director of Digital Strategy to develop a planned and coordinated online safety education programme

This will be provided through:

- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

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 to the DSL/Director of Digital Strategy for investigation/action, in line with the school safeguarding procedures
- all digital communications with pupils 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 pupils 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
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (n.b. the guidance contained in the SWGfL Safe Remote Learning Resource)
- there is 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 school and in their use of social media.

IT Service Management Provider (European Electronique)

European Electronique (EE) are responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges
- there is clear, safe, and managed control of user access to networks and devices
- 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

- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Director of Digital Strategy 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 systems are implemented and regularly updated as agreed in school policies

Pupils

- are responsible for using the school digital technology systems and their personal devices in accordance with the Pupil acceptable use agreement and Online Safety Policy
- 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 school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

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

- publishing the school Online Safety Policy on the Crosfields School app
- providing them with a copy of the Pupils' 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' online safety webinars

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

- reinforcing the online safety messages provided to pupils in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

Online Safety Group

The Online Safety Group has the following members:.

- Digital Education Governor
- Designated Safeguarding Lead
- Director of Digital Strategy

- Computing Curriculum Lead
- Head of Computing
- Head of PSHE

Members of the Online Safety Group will assist the DSL/Director of Digital Strategy with:

- the production/review/monitoring of the school Online Safety Policy
- the production/review/monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- encouraging the contribution of pupils to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Online Safety Policy

The school Online Safety 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 school and how they should use this understanding to help safeguard pupils in the digital world
- describes how the school will help prepare pupils 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 the school's policies document library
- is published on the Crosfields School app

Acceptable use

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

Acceptable use agreements

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

- staff induction and handbook
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not 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: <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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) 					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
the Computer Misuse Act (1990)	<ul style="list-style-type: none"> Gaining unauthorised access to school networks, data and files, using computers/devices Creating or 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) 					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Only acceptable for Director of Digital Strategy or DSL to access to check website content for safeguarding)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

When using communication technologies, the school considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.

- any digital communication between staff and pupils or parents/carers must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff are expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.
- users should immediately report to a member of SLT, 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.

Reporting and responding

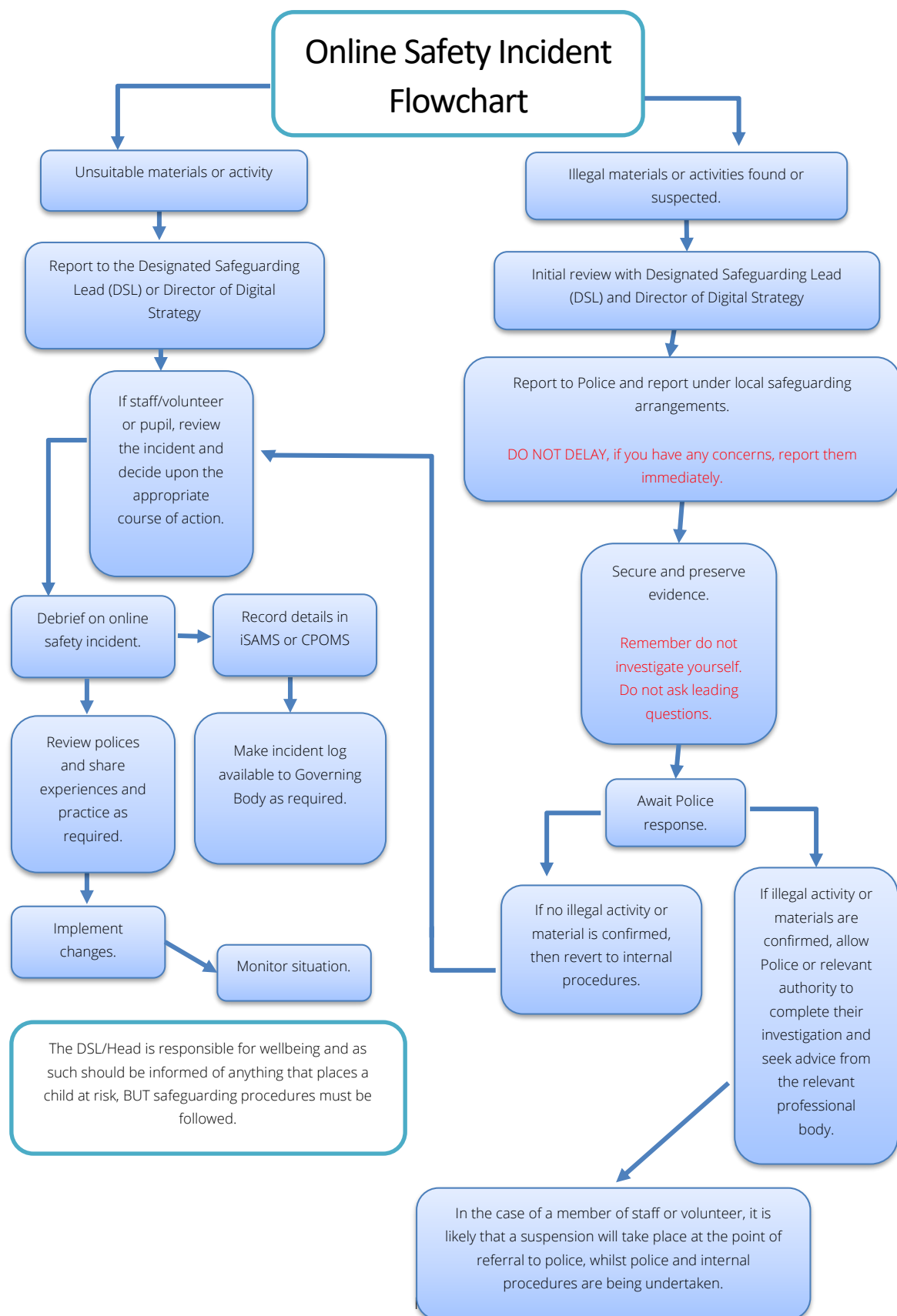
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- 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, Director of Digital Strategy 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:
 - Non-consensual images
 - Self-generated 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 Head, unless the concern involves the Head, in which case the complaint is referred to the Chair of Governors

- where there is no suspected illegal activity, devices may be checked using the following procedures:
 - one or more SLT members 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 pupils 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 screen captures 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 on iSAMS as an online safety concern and CPOMS if the incident is deemed to be a safeguarding risk
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- 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:
 - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
 - staff, through regular briefings
 - pupils, through assemblies/lessons
 - parents/carers, through the Crosfields School app

- governors, through regular safeguarding updates
- external agencies

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



School actions

It is more likely that the school 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.

Online Safety Education Programme

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against SWGfL Project Evolve and regularly taught in a variety of contexts.
- lessons are matched to need; are age-related and build on prior learning
- lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- pupil need and progress are addressed through effective planning and assessment
- digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to Pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- pupils should be helped to understand the need for the Pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- where pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites the young people visit

- it is accepted that from time to time, for good educational reasons, pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Pupils

The school acknowledges, learns from, and uses the skills and knowledge of pupils in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass pupil feedback and opinion
- appointment of digital leaders

Staff/volunteers

All staff will 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 and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by an external provider
- participation in school training / information sessions for staff or parents

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Families

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the Pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by Pupils leading sessions at parent/carer evenings.
- high profile events / campaigns e.g. Safer Internet Day
- *reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers.*

Technology

Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and European Electonique and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding staff and the IT Services Team to be effective. The DSL will have lead responsibility for safeguarding and online safety and European Electonique will have technical responsibility.

Checks on the filtering and monitoring system are carried out by European Electronique with the involvement of the Director of Digital Strategy and the DSL, in particular when a safeguarding risk is identified, there is a change in working practice or new technology is introduced.

Filtering

- the school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre.
- illegal content (e.g., child sexual abuse images) is filtered by the filtering provider by actively employing the Internet Watch Foundation URL 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, recognising that no system can be 100% effective.
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead and Director of Digital Strategy to breaches of the filtering policy, which are then acted upon.
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

Monitoring

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

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- there are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.

- management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre appropriate monitoring guidance and protects users and school systems using the appropriate blend of strategies:

- 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 school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems.
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Mobile technologies

The school acceptable use agreements for staff, Pupils, parents, and carers outline the expectations around the use of mobile technologies.

School owned/provided devices:

- all school devices are managed through the use of Mobile Device Management software.
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed.
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from school is clearly defined and expectations are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils 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 pupils, parents/carers

School staff should ensure that:

- No reference should be made in social media to pupils, 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.
- the 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 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images
- staff/volunteers must be aware of those pupils 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 is 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 pupils 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 pupils are appropriately dressed
- pupils must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with Online Safety Policy
- pupils' 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 pupils 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
- pupils' work can only be published with the permission of the Pupil 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

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 pupil work, images or videos are published, their identities are protected, and full names are not published.

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 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 it was collected for. The school '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
- 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 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

- understands 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. In order 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
- provides 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.
- device will be password protected.
- 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 safe keeping 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.