St Swithun's School Winchester

This policy applies to St Swithun's Senior School, St Swithun's Prep School and the Early Years Foundation Stage

Online Safety

Policy History	
Reviewed and updated	September 2024
Date of next review	August 2025

Reviewed by:

Deputy head (pastoral) and DSL Graham Yates Date: September 2024	Deputy Head and DSL Prep School Kate Grosscurth Date: September 2024
Head of IT Services Andy Healy Date: September 2024	Nominated Governor and School Council ratification Warwick Hill / Education Committee Date: September / October 2024

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.

Contents

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of the school to safeguard members of our entire 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, learners, volunteers, parents, guardians 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.

The policy also applies to online safety behaviour such as cyber-bullying, which may take place outside the school, but is linked to membership of the school. The school will deal with such behaviour within this policy and associated behaviour and discipline policies, and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

The 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.

Process for monitoring the impact of the Online Safety Policy

The implementation of this policy will be monitored by the senior school deputy head (pastoral), Graham Yates, and DSL and the Prep school Deputy and DSL, Kate Grosscurth.

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity

In the future we plan to conduct:

- surveys/questionnaires of:
    - learners
    - parents and carers
    - staff

The School Council will receive a termly report, from the DSLs, on the implementation of the online safety policy which will include anonymous details of online safety incidents.

Should serious online safety incidents take place, these will be dealt with in line with the safeguarding policy and the anti-bullying policy.

Links with other policies and practices

This policy links with a number of other policies, including:

- Data protection policy
- Safeguarding and Child protection policy
- Staff Code of Conduct
- Staff IT Terms and Conditions
- Social media policy
- Behaviour policy (prep and senior)
- Anti-bullying policy (prep and senior)
- Searching, screening and confiscation policy
- Pupil IT Code of Conduct (prep and senior)
- Use of mobile phones policy (prep school)

This policy is updated annually to reflect the latest KCSIE guidance and pays due regard to the following DfE guidance:

- Working Together to Safeguard Children (2023)
- On line Safety Act 2023
- Prevent Duty Guidance: for England and Wales (2015, updated 2023)
- The Prevent duty: Departmental advice for schools and childminders (2015, updated 2023)
- The use of social media for on-line radicalisation (July 2015)

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. All staff have a key role to play in feeding back on potential issues. 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 headteachers have 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 may be delegated to the Online Safety Lead (senior school deputy head pastoral/DSL and prep school deputy head/DSL) .
- The headteacher and deputy head pastoral/prep school deputy head 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 headteachers/senior leaders are responsible for ensuring that the Online Safety Lead, 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 headteachers/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 headteachers/senior leaders will receive regular monitoring reports from the Online Safety Leads.

School Council

The School Council are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out in conjunction with the Online Safety Leads who will provide regular information about online safety incidents and monitoring reports. A member of the school council will take on the responsibility of online safety and this will include:

- regular meetings with the Online Safety Leads
- receiving regular (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
- reporting to relevant School Council meetings

Online Safety Lead

Graham Yates is the deputy head and Designated Safeguarding Lead (DSL) responsible for online safety for the senior school.
Kate Grosscurth is the deputy head and Designated Safeguarding Lead (DSL) responsible for online safety in the prep school.

The Online Safety Lead will:

- lead the Online Safety Group
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and the wider community
- 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
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- identify sources of training and advice for staff, school council, parents, carers or learners
- liaise with technical staff, pastoral staff and support staff, as relevant
- meet regularly with the online safety Member of Council to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant School council meetings
- report regularly to headteacher/senior leadership team.

Designated Safeguarding Lead (DSL) and deputy DSLs

The designated safeguarding leads have lead responsibility for safeguarding and child protection including online safety and understanding the filtering and monitoring systems in place. They will:

- Ensure that ALL staff undergo online safety training, as part of their safeguarding training at induction and that this will include an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Ensure there is regular review and open communication where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. PSHE), and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused
- Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to School Council
- Ensure that online-safety education is embedded across the curriculum in line with the statutory PSHE guidance and beyond, in wider school life

- Promote an awareness of and commitment to online-safety throughout the school community, including parents
- Communicate regularly with SLT and the safeguarding Member of Council to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.

The DSL should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers/other children
- potential or actual incidents of grooming
- online bullying
- sharing nude and/or semi-nude images
- child sexual exploitation

Heads of department

Online safety education is delivered through PSHE and IT/Computing lessons. Relevant subject leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme. This will be provided through:

- a discrete programme
- PHSE and RSE programmes
- assemblies and pastoral programmes
- Resources available to pupils, parents and staff via the student wellbeing website and The Wellbeing Hub
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

PSHE Lead

The PSHE lead will:

- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE, relationships and sex education (RSE) and health education curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.
- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.

- Assess teaching to identify where pupils need extra support or intervention through tests, written assignments or self-evaluations, to capture progress to complement the computing curriculum.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Teaching, boarding and support staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct/handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond.

Staff should also be aware of the latest DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about over-blocking, gaps in provision or pupils bypassing protections.

Boarding staff should pay particular attention to **online tutors** hired by parents. They should share the Online Tutors – Keeping Children Safe poster at parentsafe.lgfl.net to remind parents of key safeguarding principles.

School staff are responsible for ensuring that:

- they have an up-to-date 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 IT Terms and Conditions
- they immediately report any suspected misuse or problem to the DSL or deputies for investigation/action, in line with the school safeguarding procedures

- ensure students understand and follow the Online Safety Policy and Pupil IT Code of Conduct
- 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 students should be guided to sites checked as suitable for their use.
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students 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

Head of IT Services and the IT Services technical staff

The technical staff are responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Cybersecurity 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 relevant legislation
- 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 DSL for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring software/systems are implemented and regularly updated as agreed in school policies

Students

- are responsible for using the school digital technology systems in accordance with the relevant Pupil IT Code of Conduct 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.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand acceptable use and behaviour regarding the taking and or sharing of nude and semi-nude images, cyber-bullying, sexting and grooming and other relevant online issues
- Should know where to access help and support when needed (e.g. through staff, online safety education, student wellbeing website and The Wellbeing Hub)

Parents, guardians and carers

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

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

- Publishing the school Online Safety Policy on the school website
- Providing them with a copy of the Pupil IT Code of Conduct
- Seeking their permissions concerning digital images, cloud services etc
- Publishing advice and guidance relating to online safety through the parent portal
- Providing access to guidance and resources through the parent pages of The Wellbeing Hub (senior school)

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

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school

When a parent/guardian/carer supplies a student with a mobile device equipped with a mobile data SIM card, any filtering solution implemented by the school does not apply. They are therefore granting their child unfiltered/unmonitored internet access.
Prep school pupils are not permitted mobile phones/data enabled devices in school.

Community users and Guests

Community users and guests who access the guest Wi-Fi as part of the wider school provision must agree to an acceptable usage policy prior to gaining access to the school Wi-Fi.

Policy

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 learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels.
- is published to parents on the school portal.

Acceptable use

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

Acceptable use agreements

This Online Safety Policy, the Staff IT Terms and Conditions, Pupil IT Code of Conduct define acceptable use at the school. These acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- splash screens
- communication with parents/carers
- teaching sessions as appropriate
- parent portal

		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:** • 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 N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of 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) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to					X

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				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	X
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	

The school's web filtering policy can be viewed here for school staff:

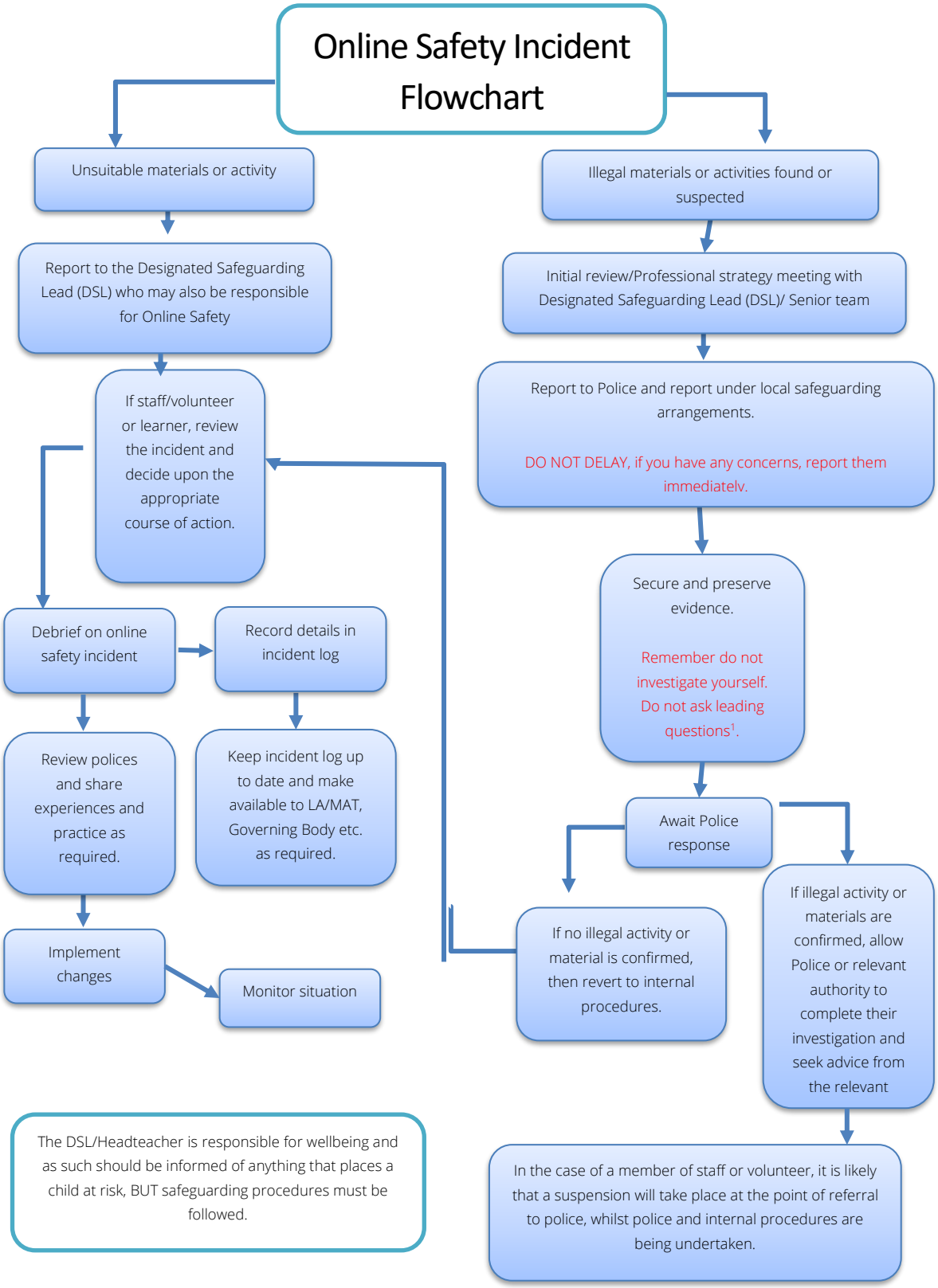
Web Filtering Policy

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 that:

- 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 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.
- 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 Chair of Governors
- where there is no suspected illegal activity, devices may be checked in line with the searching, screening and confiscation policy,
- there are support strategies in place for those reporting or affected by an online safety incident
- incidents should be logged, both on CPOMS and on an online safety incident log held by the DSL
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues,
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions

The following flowchart can be used to guide the decision-making process for dealing with online safety incidents.



Responding to Student Actions

The sorts of incidents that are most likely include:

- deliberately accessing or trying to access material that could be considered illegal
- Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords
- Corrupting or destroying the data of other users.
- Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.
- Unauthorised downloading or uploading of files or use of file sharing.
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic mate
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act
- Unauthorised use of digital devices (including taking images)
- Unauthorised use of online service
- Actions which could bring the school into disrepute or breach the integrity or the ethos of the school
- Continued infringements of the above, following previous warnings or sanctions.

Depending on the nature and context of such incidents, responses may include:

- Issue of warning
- Education about appropriate / inappropriate actions
- Referral to tutor, head of department, head of year, deputy headteachers, headteacher
- Further sanction, in line with behaviour policy
- Removal of device and/or network access
- Referral to police
- Referral to children's services

Responding to Staff Actions

The sorts of incidents that will be investigated are most likely include:

- Deliberately accessing or trying to access material that could be considered illegal
- Deliberate actions to breach data protection or network security rules
- Deliberately accessing or trying to access offensive or pornographic material
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.
- Using proxy sites or other means to subvert the school's filtering system.
- Unauthorised downloading or uploading of files or file sharing
- Breaching copyright or licensing regulations.
- 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
- Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers
- Inappropriate personal use of the digital technologies e.g. social media / personal e-mail
- Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity or the ethos of the school
- Failing to report incidents whether caused by deliberate or accidental actions
- Continued infringements of the above, following previous warnings or sanctions

Incidents will be investigated by a member of the senior leadership team in whichever school the issue arises and, depending on the outcome of the investigation, appropriate action will be taken in line with our policies and statutory requirements.

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

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 will be provided in the following ways:

- A planned online safety curriculum for all year groups. Lessons are matched to need, are age-related and build on prior learning.
- This will cover the four areas of risk within online safety:
    - Content - age-inappropriate or unreliable content can be available to children.

    - Contact - children can be contacted by bullies or people who groom or seek to abuse them.
    - Conduct - children may be at risk because of their own behaviour, for example, by sharing too much information.
    - Commerce - young people can be unaware of hidden costs and advertising in apps, games and websites.
- Digital competency is planned and effectively threaded through the appropriate elements in other curriculum areas
- To incorporate and make use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.

Staff

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- all new staff will receive online safety training (including data protection 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.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- Online safety training will be delivered through staff meetings as required

Parents/guardians/carers

Parents, guardians and carers play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

In light of this, the school will seek to provide information and awareness to parents and carers through communication, awareness-raising and engagement on online safety issues through signposting to relevant resources on the Parent Portal and the senior school Wellbeing Hub.

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

We pay due regard to the DfE guidance 'Meeting digital and technology standards in schools and colleges 2023'

Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined both in the UK Safer Internet Centre Appropriate filtering document and the DfE's 'Meeting digital and technology standards in schools and colleges 2023'
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- the school has provided enhanced/differentiated user-level filtering, allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/students/guests, etc.
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- 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.
- a member of Internet Watch Foundation (IWF)
- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- blocking access to illegal content including child sexual abuse material (CSAM)

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.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- 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
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These include:

- 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

Technical Security

See IT Technical Security Policy

Social media

See Social Media policy

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:

- staff must be aware of those learners whose images must not be taken/published. All images should only be taken on school devices.
- The personal devices of staff should not be used for any such purposes as outlined in the staff code of conduct
- staff 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
- 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.
- images will be securely stored in line with the school retention policy

Data Protection

See Data Protection policy

Artificial Intelligence

Artificial Intelligence (AI) tools are becoming increasingly prevalent and have a wide-ranging impact on education. There are obvious concerns and nervousness regarding use of AI including data privacy, security, academic dishonesty and exam integrity. Equally, Large Language models (LLM) such as ChatGPT can be a powerful aid for research and assignments. These same tools can potentially generate entire pieces of work and the challenge for staff is to identify such submissions as plagiarism. Students should not rely on AI to complete their work but, instead, could use it as a personal tutor, when permitted by the teacher. They should also be aware that LLMs are not fool-proof and should cross-check AI responses for accuracy. Correct use of AI is taught as part of PSHE and Computing lessons. Misuse of AI will be treated in line with the school's behaviour policy.