



Introduction

The DfE Keeping Children Safe in Education statutory guidance requires schools in England to ensure that learners are safe from harm:

*"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to **online safety** empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate"*

*"Governing bodies and proprietors should ensure **online safety** is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how **online safety** is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement"*

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

2 Scope of Policy

This Online Safety Policy applies to all members of the school community- including staff, pupils and volunteers who have access to and are users of the school digital systems, both in and out of school.

It is applied to the use of personal digital technology on the school site (where allowed).

Holme Court School will deal with such incidents within this policy and associated behaviour and antibullying practices and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place both in and outside of school.

This policy is made available to staff at induction and through normal communication channels.

An electronic version is available via the school SharePoint/Staff/Staff/policies. It is published on the school website.
A hard copy is available from the school admin office.

3 Policy statement

At Holme Court School we believe that pupils should be able to access the internet and digital technologies for educational and personal development without experiencing abuse of any kind. However, in order to keep pupils safe, it is essential that safeguards are put in place.

We recognise that:

- the online world provides everyone with many opportunities but can also present risks and challenges
- we have a duty to ensure that all pupils and adults involved in our community are protected from potential harm online
- we have a responsibility to help keep pupils safe online whether or not they are using Home Court school's network and devices
- working in partnership with pupils, their parents/carers and other agencies is essential in promoting young people's welfare and in helping our pupils to be responsible in their approach to online safety
- all pupils have the right to equal protection from all types of harm or abuse

4 Legislative-statutory compliance

This policy agreement has due regard to all relevant legislation and statutory guidance including, but not limited to the following:

Legislation

- The UK General Data Protection Regulation (UK GDPR)
- Protection of Freedoms Act
- The Freedom and Data Protection (Appropriate Limit and Fees) Regulations 2024
- Freedom of Information Act 2000
- The Education (pupil Information) (England) Regulations 2005 (as amended in 2018)
- The Data Protection Act 2018 (DPA)
- Counter Terrorism and Securities Act 2015
- School Standards and Framework Act 1998

Guidance

- Keeping Children Safe in Education -DfE (2025)
- Technical Guidance for Schools In England - Equality and Human Rights Commission (2024)
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)
- Data Protection: A toolkit for schools- DfE (2018)

5 Aims of Policy

The Holme Court School Online Policy sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.

It:

- clarifies responsibilities for the delivery of the policy
- 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

This policy is supplemented by a series of related Acceptable Use Agreements (AUAs).

6 Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of our 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.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding
- The headteacher and Safeguarding Team members 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 headteacher/senior leaders are responsible for ensuring that the DSL, Deputy Safeguarding Leads (DDSLs), 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 allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Deputy Designated Safeguarding Lead/Business Manager.
- The headteacher/DSL and DDSL/Business Manager will work with the Proprietor and IT service providers in all aspects of filtering and monitoring.

The Proprietor

The DfE guidance "Keeping Children Safe in Education" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare this includes ... online safety"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. 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)"

- The proprietor is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

In relation to this, the Proprietor will:

- receive regular information about online safety incidents and monitoring reports.
- Attend termly meetings with the Designated Safeguarding Lead / Online Safety Lead
- receive termly (collated and anonymised) reports of online safety incidents
- check that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- The Proprietor will ensure 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, DDSL/Business Manager, the Director of Finance and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- The proprietor will receive basic cyber-security training to enable her to check that the school meets the DfE Cyber-Security Standards
- The Proprietor will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

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"

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 her to understand the risks associated with online safety and be confident that she has the relevant knowledge and up to date capability required to keep children safe whilst they are online#
- meet regularly with the Proprietor in her role as 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

- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded
- liaise with staff and IT providers on matters of safety and 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)
- 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/the Proprietor/parents/carers/learners
- 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 learners) 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/OSL to develop a planned and coordinated online safety education programme

This will be provided through:

- a discrete programme
- PSHE and SRE programmes
- A mapped Cross-Curricular programme
- Assemblies
- 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 follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with pupils, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements)
- they immediately report any suspected misuse or problem to The DSL/ Business Manager for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- 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
- 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 (n.b. the guidance contained in the SWGfL Safe Remote Learning Resources)
- 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
- they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated

IT Provider

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 IT service provider should have technical responsibility for:

- *maintaining filtering and monitoring systems*
- *providing filtering and monitoring reports*
- *completing actions following concerns or checks to systems"*

"The IT service provider should work with the senior leadership team and DSL to:

- *procure systems*
- *identify risk*
- *carry out reviews*
- *carry out checks"*

The IT Provider is 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 and guidance from local authorities that the school works with
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) 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 (see appendix 'Technical Security Policy template' for good practice).
- monitoring systems are implemented and regularly updated as agreed in school policies

Pupils

Pupils are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this includes personal devices – where allowed)

Pupils should:

- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know what to do if they or someone they know feels vulnerable when using online technology
- avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services
- 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

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 learners' acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- publishing information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc (see parent/carers AUA in the appendix)
- 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)

7 Professional standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms

- Where Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.

8 Acceptable use

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

Acceptable Use agreements

An acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. At Holme Court School there are separate agreements in place for pupils, parents and staff and visitors.

The Acceptable Use Agreements will be communicated/re-enforced through:

- The staff induction and handbook
- Signing of agreements by staff, pupils and parents
- IT curriculum
- PSHE curriculum
- Assemblies
- Internet safety curriculum days
- Form discussions

Pupil and parent/carers AUAs are available on the school website.

To support pupils, parents and staff the school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including	Any illegal activity for example: <ul style="list-style-type: none"> • Child sexual abuse imagery 					X

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
<p>apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:</p>	<ul style="list-style-type: none"> • 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 • Identity fraud • Impersonating official bodies <p>N.B. The schools will refer to the following guidance about dealing with self-generated images/sexting - UKSIC Responding to and managing sexting incidents and UKCIS - Sexting in schools and colleges</p>				
<p>Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)</p>	<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) • 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) • Disabling/Impairing/Disrupting the network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) 				X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Serious or repeat offences should be reported to 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	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 and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				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 (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be 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 nominated person – in accordance with the school 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.
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

9 Reporting

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. 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:

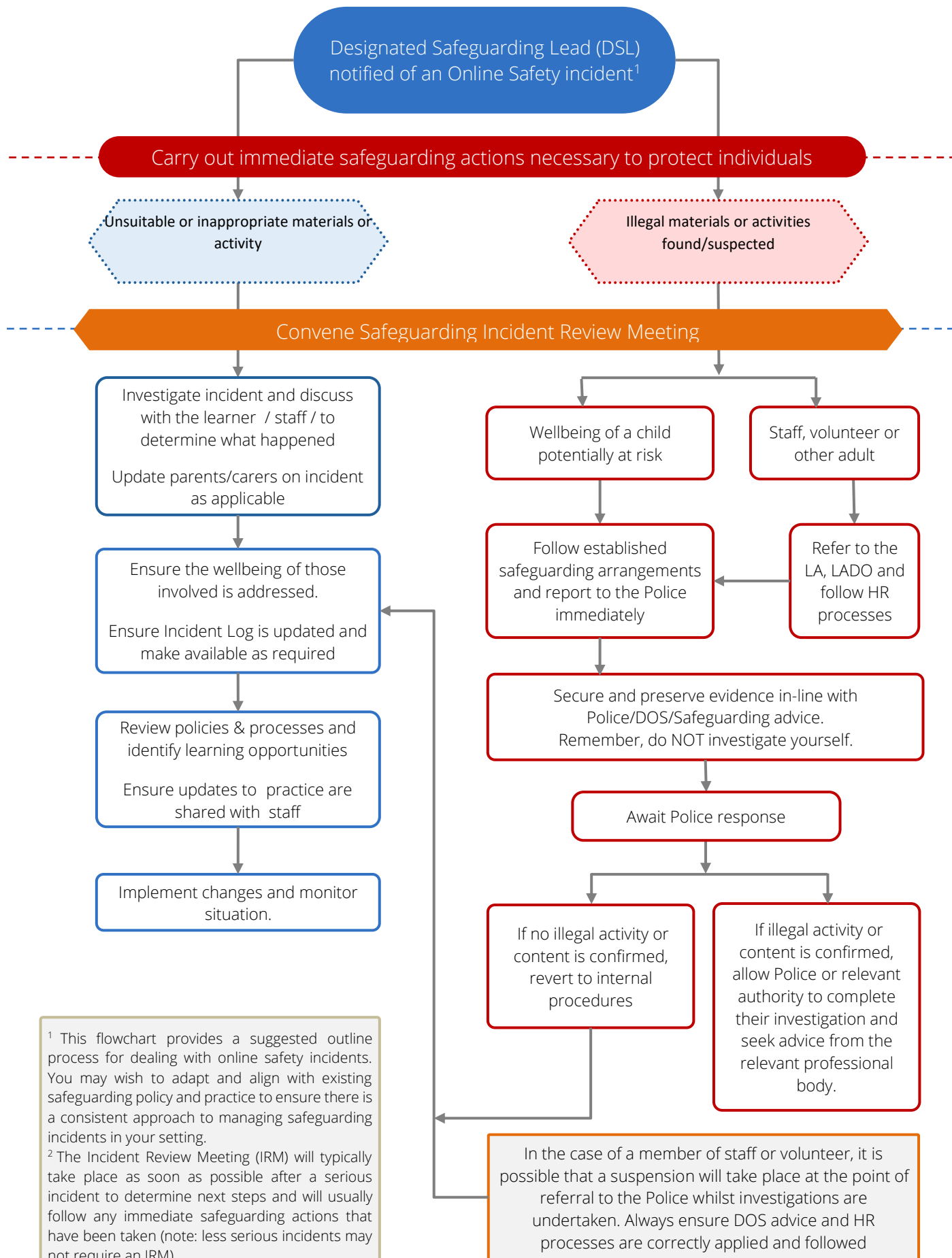
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school

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 ([see flowchart and user actions chart in the appendix](#)), 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 Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Proprietor
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- 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
 - involvement by local authority
 - 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 under the welfare tab on Behaviour Watch
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; 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 (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - staff, through regular briefings
 - learners, through assemblies/lessons
 - parents/carers, through newsletters, school social media, website
 - the Proprietor, through regular safeguarding updates
 - local authority/external agencies, as relevant (*The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"*)

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



¹ This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

² The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

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 as follows:

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Headteacher	Refer to Police/Social Work	Refer to Kyonet for technical support for advice/action	Inform parents/carers	Remove device/network/internet access	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).	X	X	X	X	X	X		X
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	X	X		X	X	X	X	
Corrupting or destroying the data of other users.	X	X		X	X	X	X	
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	(X)		X	(X)	X	X
Unauthorised downloading or uploading of files or use of file sharing.	X	X		X	X	X	X	

Using proxy sites or other means to subvert the school's filtering system.	X	X		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	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X			X		X	
Unauthorised use of digital devices (including taking images)	X	X			X		X	
Unauthorised use of online services	X	X		X	X		X	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X		X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X	(X)	X	X	X		X

10 The use of AI systems in school

Please see separate AI Policy.

11 Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils 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.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."

Keeping Children Safe in Education states:

"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum ..."

At Holme Court School, we advocate that 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 a nationally agreed framework and regularly taught in a variety of contexts where:

- 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
- digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g Internet safety day, Anti-Bullying week
- the programme is be accessible to pupils at different ages and abilities
- pupils are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- pupils are taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse
- Pupils are 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 act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils 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 pupils are allowed to freely search the internet, staff are vigilant in supervising the pupils and monitor the content of the websites / tools (including AI systems) the pupils 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.

	School devices			Personal devices		
	School owned for individual use Staff	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	No	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Na	Yes		No	No	Yes

12 Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- *the school permits reasonable and appropriate access to personal social media sites during school hours*

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.

See Social media policy for more detail.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying 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:

- 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 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 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. (see parents and carers acceptable use agreement). Permission is not required for images taken solely for internal purposes
- 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-Facebook
- Online newsletters

The school website is managed/hosted by the Business Manager. 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.

13 Monitoring of policy

The school will monitor the impact of this policy using:

- Filtering and monitoring logs
- Surveys/questionnaires of pupils and staff
- Welfare concerns raised

14 links to other policies-documentation

AI policy

Anti-bullying Policy

Behaviour Policy

Data Security Policy

Safeguarding /Child Protection Policy

Disciplinary Policy and Procedure

Agreements

Staff and volunteer acceptable use agreement

Pupil Acceptable Use Agreement

Parent/carer Acceptable Use Agreement

15 version control

Version	Comments	Reviewer
1.0	April 2025	Anita Laws