Our Lady of Good Help

Catholic Primary School

Online Safety Policy

Chair of Governors	Mrs S. Devereux
Headteacher	Mr M. McQuiston
Date adopted: September 2023	**Review Date:** September 2024

'Like Our Lady, we live wisely, think deeply and love generously in Christ.'

Contents

1. Introduction

At Our Lady of Good Help, we recognise the ever-changing and growing influence of technology in our daily lives. We recognise our duty in ensuring pupils attending our school, and the staff who teach our pupils, are taught to use technology responsibly and respectfully and, although we recognise the benefits of this technology, we must also be aware of the potential risks.

Some of the potential dangers of using technology include but not limited to:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to/ loss of/ sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing/ distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/ contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video/ internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure 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"*

The DfE Keeping Children Safe in Education guidance also recommends:

> *'Reviewing online safety … Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the 360 safe self-review tool'*

1.1 Scope of the Online Safety Policy

This policy aims to meet our statutory obligations to ensure that learners are safe and are protected from potential harm, both on and off-site. It will also form part of the school's protection from legal challenge,

relating to the use of digital technologies. It is intrinsically linked to other relevant policies such as a school's Child Protection Policy, Behaviour & Relationship Policy and Anti-Bullying Policy. The school will use this policy, and other related policies, when investigating incidents/ allegations of inappropriate online behaviour that takes place inside and outside of school and will inform parents/ carers as part of this process.

1.2 Process for monitoring the impact of the Online Safety Policy

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 (MGL technical support)
- surveys/questionnaires of:
    - pupils and staff
    - parents and carers

2. 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.

<u>Headteacher and Assistant Headteacher</u>

- 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 Assistant Headteacher must 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 and Assistant Headteacher are responsible for ensuring that the Computing 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 Headteacher and Assistant Headteacher 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 will receive Smoothwall notifications of any unwanted online activity and a summary email from Smoothwall once a week.

<u>As DSL (Also HT):</u>

- 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 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.
- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments.
- Provide or identify sources of training and advice for staff/ governors/ parents/ carers/ pupils.
- Liaise with MGL technical staff, pastoral staff and support staff when necessary.
- Meet with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs.
- Attend relevant governing body meetings.
- Liaise with the local authority.

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

> *"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety). This should be explicit in the role holder's job description." … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … 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."*

<u>Governors</u>

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"

Governors are 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'.**

This review will be carried out by the Governor Wellbeing 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 Computing Lead
- 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
- reporting to relevant governors
- occasional review of the filtering change control logs and the monitoring of filtering logs (where

possible)

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

Curriculum Leads

The Assistant Headteacher will work with the Computing Lead and RSHE Lead to develop a planned and coordinated online safety education map. This will be provided through:

- Sequenced online safety lessons through RSHE and computing sessions.
- Planned assemblies and pastoral programmes.
- Taking part in relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- Responding to the needs of the school, when required.

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.
- They immediately report any suspected misuse or problem to the DSL, in line with the school safeguarding procedures.
- All digital communications with pupils and parents/ carers should be 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 and implement current policies regarding these devices.
- In lessons where internet use is pre-planned, 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource.
- 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.

Network Manager/ Technical Staff

The network manager/ technical staff (MGL) is responsible for ensuring that:

- They are aware of and follow the school Online Safety 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 local authority or other relevant body .
- 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 the DSL.
- The Firewall and 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.

Pupils

Pupils need to know and understand that they:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement and Online Safety Policy (this should include personal devices – where allowed).
- Should report abuse, misuse or access to inappropriate materials and know how to do so.
- Should tell a trusted adult if they or someone they know feels vulnerable when using online technology.
- Should adopt 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/ 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 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'/ carers' evenings, newsletters, website, social media and information about national/ local online safety campaigns and literature.

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

- Reinforcing the online safety messages provided to pupils in school.
- Ensuring pupils comply with the school's policy on personal devices.

Community Users

Community users who access the school systems/ website/ or learning platforms, as part of the wider school provision, will be expected to sign a Community User Acceptable Use Agreement before being provided with access to school systems.

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

3. Policy

3.1 The 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 on the school website.

3.2 Acceptable Use Agreements

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 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 the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information here					X

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 or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes onsite:	Pupils				Staff			
	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	**X**				**X**			
Online shopping/commerce	**X**						**X**	
File sharing			**X**			**X**		
Social media	**X**						**X**	
Messaging/chat	**X**						**X**	
Entertainment streaming e.g. Netflix, Disney+	**X**						**X**	
Use of YouTube (EG. FOR LEARNING PURPOSES)	**X**						**X**	
Mobile phones may be brought to school				**X**		**X**		
Use of mobile phones for learning at school	**X**				**X**			

Use of mobile phones in social time at school (EG. STAFF ROOM)	X					X		
Taking photos on mobile phones/cameras	X				X			
Use of other personal devices, e.g. tablets, gaming devices	X				X			
Use of personal email in school	X						X	
Connecting personal devices to the school WIFI	X				X			
Use of school email for personal emails	X				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 (email, social media, learning platform, etc.) must be professional in tone and content. Personal email 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.

3.3 Reporting and Responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

> "School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:

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

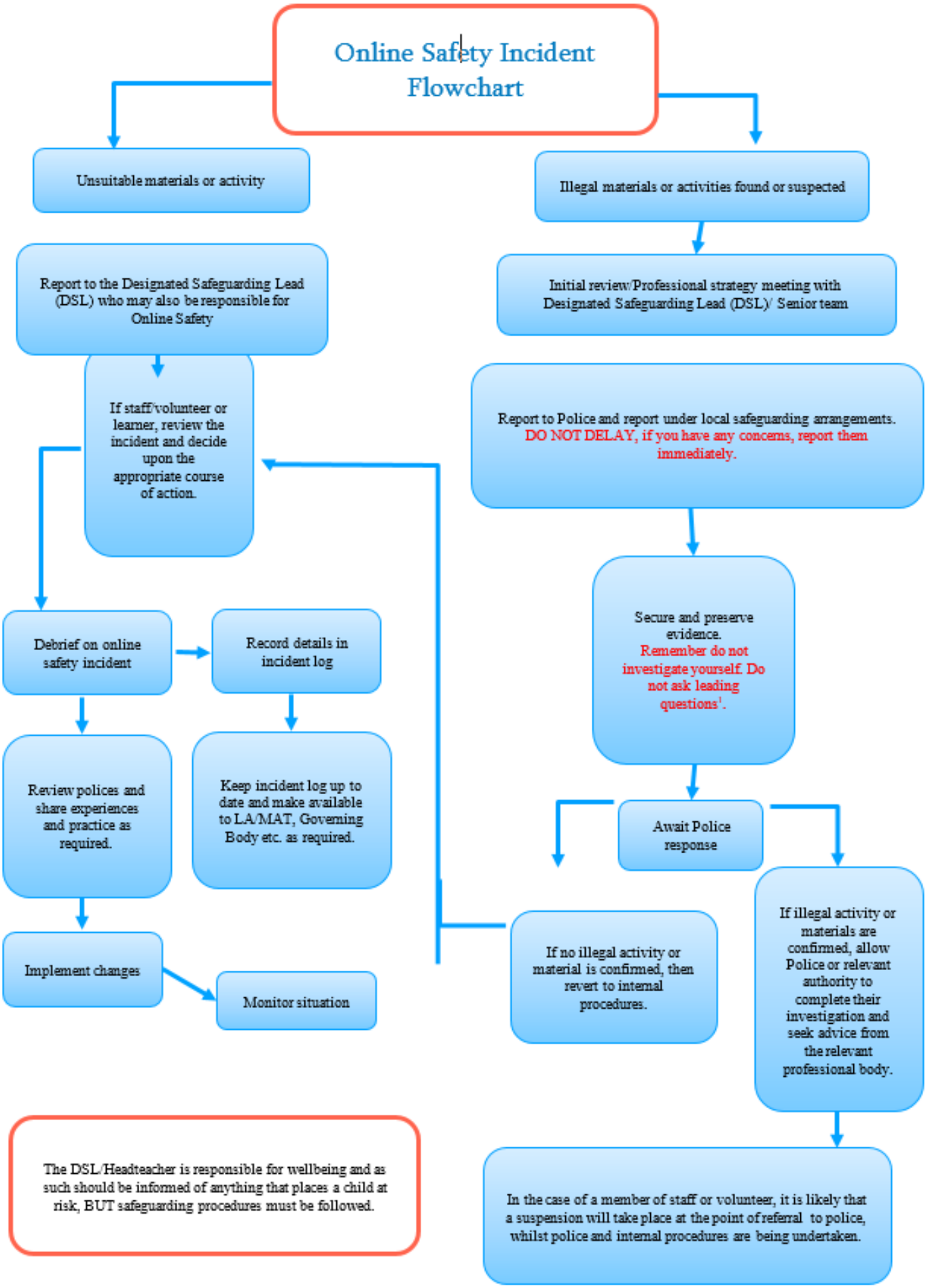
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/ incidents.
- Reports will be dealt with as soon as is practically possible once they are received .
- The Designated Safeguarding Lead 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.
- 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 and the Local Authority Designated Officer.
- 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 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 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 (as relevant)
        - 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 CPOMs.

- 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:
    - HT/ DSL for consideration of updates to policies or education programmes and to review how effectively the report was dealt with;
    - staff, through regular briefings;
    - learners, through assemblies/lessons;
    - parents/carers, through newsletters, school social media, website;
    - governors, through regular safeguarding updates;
    - local authority/external agencies, as relevant.

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

3.4 Online Safety Incident Flowchart



3.5 Responding to Learner 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:

Incidents	Refer to class teacher	Refer to Assistant Head	Refer to HT	Refer to Police/ Social Work	Refer to MGL for advice & action	Inform parents/ carers	Remove device/ network/ internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal.		X	X	X		X			X
Attempting to access or accessing the school network, using another user's account (staff or pupil) or allowing others to access school network by sharing username and passwords	X	X	X			X		X	
Corrupting or destroying the data of other users.		X	X			X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			X			X
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
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		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
Continued infringements of the above, following previous warnings or sanctions.			X			X	X		X

All incidents will be judged on their own individual merits and decisions made will be proportionate to the offence.

3.6 Responding to Staff Actions

Incidents	Refer to line manager	Refer to HT	Refer to HR	Refer to Police	Refer to MGL Technical Support	Warning	Suspension	Further Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal.		X	X	X			X	X
Deliberate actions to breach data protection or network security rules.		X	X	X			X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X			X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X			X	X
Using proxy sites or other means to subvert the school's filtering system.		X	X	X			X	X
Unauthorised downloading or uploading of files or file sharing	X	X	X			X	X	X
Breaching copyright or licensing regulations.	X	X				X		
Allowing others to access the school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X	X			X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x	x		x	x	x
Using personal email/social networking/messaging to carry out digital communications with learners and parents/carers	x	x	x			x	x	x
Inappropriate personal use of the digital technologies e.g. social media / personal email	x	x	x			x	x	
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	x	x	x			x	x	x
Actions which could compromise the staff member's professional standing	x	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
Failing to report incidents whether caused by deliberate or accidental actions		x	x			x	x	x
Continued infringements of the above, following previous warnings or sanctions.		x	x				x	x

All incidents will be judged on their own individual merits and decisions made will be proportionate to the offence.

3.7 Online Safety Education

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.
- 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 needs 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 e.g. RSHE, RSE, Computing, English etc.
- It incorporates 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.
- 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.
- Staff should 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 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.

For further information, please see the Computing and RSHE curriculums.

4. Other Associated Policies

The school has a range of associated policies and procedures linked to online safety:

- Child Protection Policy
- Safer Working Practices (Code of Conduct) Policy
- Behaviour & Relationships Policy
- Anti-bullying Policy
- Acceptable Use Agreement Policy
- Computing Policy
- Social Media Policy
- Firewall & Filtering Policy
- Digital Images and Video Policy
- Data Protection Policy
- Mobile Phone Policy

5. Outcomes

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

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