Online safety policy

FREQUENCY OF REVIEW:	**Annually**
RATIFICATION:	**Autumn 2023**
APPROVED BY:	**Local Governing Body**
DATE OF NEXT REVIEW:	**Autumn 2024**
AUTHOR:	**Assistant Headteacher (Online safety co-ordinator)**

Contents

Scope of the Online Safety Policy

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

The DfE (Department for Education) Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure Students 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.

The DfE Keeping Children Safe in Education guidance suggests that:

> The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:
>
> **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
>
> **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
>
> **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g., consensual, and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

This Online Safety Policy applies to all members of the school community (including staff, Students, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. The use of personal devices is not allowed, except in circumstances that are agreed by a member of SLT, in these exceptional circumstances the policy applies to the use of personal digital technology on the school site.

Church Stretton 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.

Policy development, monitoring, and review

This Online Safety Policy has been developed through consultation with relevant stakeholders, made up of:

- Senior leaders.
- Designated safeguarding lead (DSL).
- Online Safety lead (OSL).
- Staff – including teachers/support staff/technical staff.
- Governors

Schedule for development, monitoring, and review.

This Online Safety Policy was approved by the school governing body on:	12.10.2023
The implementation of this Online Safety Policy will be monitored by:	Dan Bird, Online Safety Co-ordinator
Monitoring will take place at regular intervals:	Once per academic year
The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Once per academic year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Autumn term 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Executive Headteacher, Head of School, Designated Safeguarding Lead, and the Safeguarding Governor. They will determine the course of action to be taken. If the issue involves safeguarding concerns, then the School's Safeguarding policy will be followed to determine whether to inform external persons/agencies.

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)/filtering.
- internal monitoring data for network activity.
- surveys/questionnaires of:
    - Students,
    - parents and carers,
    - staff.

Roles and 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.

Executive Headteacher, Head of School and senior leaders

- The Head of School has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Head of School, Online Safety Co-ordinator and Designated Safeguarding Leads 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 (Appendix 1).
- The Head of School is responsible for ensuring the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Head of School 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 Church Stretton School SLT will receive regular monitoring reports from the Online Safety Co-ordinator.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the nominated Safeguarding Governor who takes on the role of Online Safety Governor to include:

- Review meetings with the Designated Safeguarding Lead / Online Safety Lead
- Regularly receiving (collated and anonymised) reports of online safety incidents
- Regular monitoring of filtering/change control
- reporting to relevant *governors group/meeting*

Designated Safeguarding Lead (DSL)

- Hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Meet regularly with the online safety lead and Safeguarding Governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- Attend relevant governing body meetings.
- 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, safeguarding, and welfare (including online and digital safety).

Online Safety Lead

- 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 on CPOMS 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 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 training and advice for staff/governors/parents/carers/Students.
- Liaise with the Network Manager, Telford and Wrekin IT and the Trust
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by Students) regarding 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:

- Computer Science curriculum.
- PCHSE curriculum.
- Assemblies and pastoral programmes.
- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices.
- They understand that online safety is a core part of safeguarding.
- They have read, understood, and agreed to the IT acceptable use policy.
- They immediately report any suspected misuse or problem to the DSL using CPOMS for investigation/action, in line with the school safeguarding procedures.
- All digital communications with Students and parents/carers are on a professional level *and only carried out using official school systems as per the IT acceptable use policy.*
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure Students 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.
- In lessons where internet use is pre-planned Students 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.*
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Manager

The IT Manager is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required e-safety technical requirements.
- Users may only access the networks and devices through a properly enforced password protection policy, which meets sufficiently high complexity requirements, as well as being checked against known passwords.
- The filtering is applied and updated on a regular basis.
- They keep up to date with e-safety technical information to effectively carry out their e-safety role and to inform and update others as relevant.
- The use of the network is regularly monitored in order that any misuse or attempted misuse can be reported to the Online Safety Lead.
- Monitoring software and systems are kept up to date.

IT Provider

Telford and Wrekin IT services have technical responsibility for:

- Maintaining filtering and monitoring systems.
- Providing filtering and monitoring reports.
- Completing actions following concerns or checks to systems.

Telford and Wrekin IT services should work with the Network Manager, senior leadership team and DSL to:

- Procure systems.
- Identify risk.
- Carry out reviews.
- Carry out checks.

Telford and Wrekin IT services 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 DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from the Trust.
- 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 Evan Morgan, Network Manager, for investigation and action.

- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Monitoring systems are implemented and regularly updated.

Students

- Are responsible for using the school digital technology systems in accordance with the student IT acceptable use policy and Online Safety Policy.
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

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 IT Acceptable Use Policy.
- Publishing information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images etc.
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

- reinforcing the online safety messages provided to Students in school.

Community Users, Visitors and Volunteers

Community Users, visitors and volunteers who require access to School systems are given access to the internet via their own device using a Wi-Fi code (access to school drives/data is restricted) or access to a desktop with the appropriate level of permissions – starting at internet access only.

Professional Standards

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

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 students in the digital world.
- Describes how the school will help prepare students 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, through staff meetings, CPD (Continuing Professional Development) and shared via an emailed link.
- Is published on the school website.

Acceptable use

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

Acceptable use agreements

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

- Staff induction and handbook.
- Digital signage.
- Posters/notices around where technology is used.
- Communication with parents/carers.
- Built into education sessions.
- School website.

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.					**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, using computers/devices. • Creating or propagating computer viruses or other harmful files. • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords). • Disable/Impair/Disrupt network functionality using computers/devices. • Using penetration testing equipment (without relevant permission).					**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.			X	X	
	Promotion of any kind of discrimination.				X	
	Using school systems to run a private business.				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Using systems, applications, websites, or other mechanisms that bypass the filtering/monitoring 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	

Internet/Device use	Staff and other adults				Students			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
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 video broadcasting, e.g., YouTube, Twitch, TikTok	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		X			X			
Taking photos on mobile phones/cameras	X				X			
Use of other personal devices, e.g., tablets, laptop, Chromebook		X						X
Use of personal e-mail in school, or on school network/wi-fi			X		X			
Use of school e-mail for personal e-mails	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 Students 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.
- Staff should not refer to Church Stretton School on any of their social media accounts.
- 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 Students.*

Reporting and responding

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

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The Designated Safeguarding Lead, 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 (Appendix 1), 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 Executive Headteacher using Staff Safe, unless the concern involves the Executive Headteacher, in which case the complaint is referred to the Chair of Governors and the Trust.
- 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 students 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).

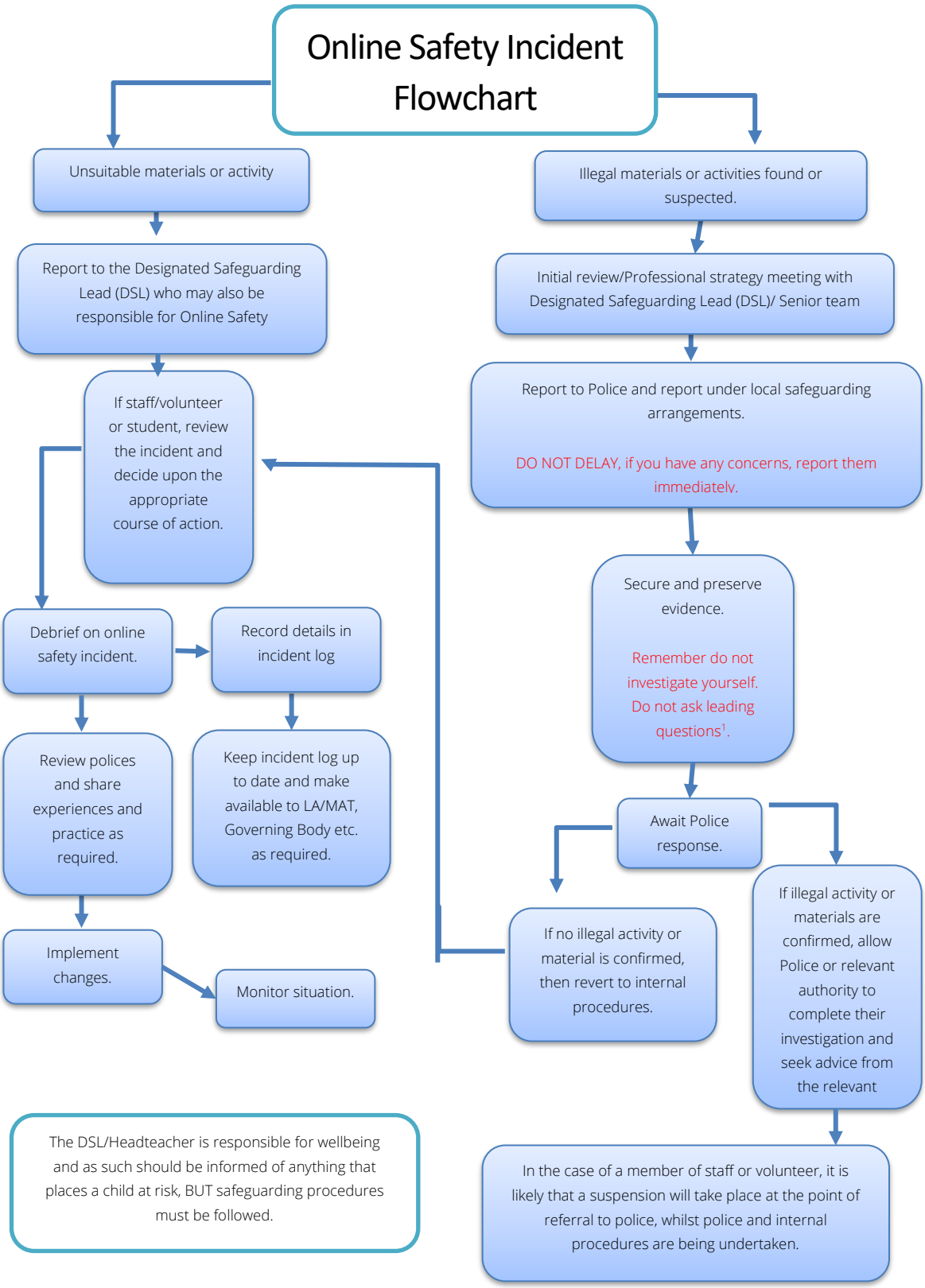
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.
- Once this has 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 of the Trust.
    - 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, student concerns, or Staff Safe, staff concerns.
- 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:
    - The Online Safety Lead for consideration of updates to policies or education programmes and to review how effectively the report was dealt with.
    - Staff, through regular briefings.
    - Students, through assemblies/lessons.
    - Parents/carers, through newsletters, school social media, website.
    - Governors, through regular safeguarding updates.
    - The Trust/external agencies, as relevant.

- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes. The school will make the flowchart below (Appendix 1) available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or student, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediatelv.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Allegations and Sanctions

Safeguarding allegations or concerns about Staff will be handled in accordance with the Safeguarding and Protecting Children Policy and Procedures. Staff misuse of School ICT (Information and Communication Technology) systems will be dealt with in accordance with the Disciplinary and Dismissal Procedure.

Pupils' misuse of School ICT systems will be dealt with in accordance with the School's Behaviour, Rewards, Discipline and Sanctions Policy.

Online Safety Education Programme

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

- A planned online safety curriculum for all year groups matched against a nationally agreed framework SWGfL Project Evolve and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Student need and progress are addressed through effective planning and assessment.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas.
- It incorporates/makes use of relevant national initiatives and opportunities e.g., Safer Internet Day and Anti-bullying week
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND (Special Educational Needs and Disabilities).
- Students should be helped to understand the need for the student 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 students 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 Students are allowed to freely search the internet, staff should be vigilant in supervising the students and monitoring the content of the websites the young people visit using Senso.
- 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 obvious reasons for the need.
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Staff/volunteers

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

- A planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- The training will be an integral part of the school's annual safeguarding and data protection training for all staff.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation, and the need to model positive online behaviours.
- The Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions. This will be offered through participation in school and online training.

A higher level of training will be made available to the Safeguarding Governor. This will include:

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

Families

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

- *Regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes.*
- *Regular opportunities for engagement with parents/carers on online safety issues through parent/carer evenings.*
- *The students – who are encouraged to pass on to parents the online safety messages they have learned in lessons.*
- *Letters, newsletters, website, learning platform links to high profile events / campaigns.*
- *Sharing good practice with other schools in the Trust.*

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.

Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider, Telford and Wrekin IT services, and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

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

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the DSL, a governor, and the IT manager with the involvement of Telford and Wrekin IT services.

- Checks on the filtering and monitoring system are carried out by Telford and Wrekin IT services with the involvement of a senior leader, the DSL, a governor, and the IT manager, in particular when a safeguarding risk is identified, there is a change in working practice, e.g., remote access or new technology is introduced.

Filtering

- The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided, Smoothwall filtering, meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).

- Filtering logs are regularly reviewed and alert the DSL to breaches of the filtering policy, which are then acted upon.

Monitoring

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

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

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems using the appropriate blend of strategies 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.
- Use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s).

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- Responsibility for technical security resides with SLT who may delegate activities to identified roles.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Manager and Telford and Wrekin IT services and will be reviewed, at least annually, by the SLT.
- Password policy and procedures are implemented.
- The security of their username and password and must not allow other users to access the systems using their log on details.
- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- The administrator passwords for school systems are kept in a secure place, e.g., school safe.
- There is a risk-based approach to the allocation of student usernames and passwords.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems, and cabling are securely located and physical access restricted.
- Appropriate security measures are in place through our IT service provider Telford and Wrekin IT services to protect the servers, firewalls, routers, wireless systems, and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- Evan Morgan is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them.
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- Staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider.

- Removable media is not permitted unless approved by the SLT/IT service provider.
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See school personal data policy template in the appendix for further detail)
- Mobile device security and management procedures are in place. Students are not permitted to use mobile devices in school and two factor authentication is in use on staff and student accounts when used on mobile devices.
- Guest users are provided with appropriate access to school systems based on an identified risk profile.

Mobile technologies

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

Due to the rural location of the school the school allows mobile devices in school as long as students:

- Keep their phone in their bag.
- Have their phone turned off.
- There may be exceptions to these rules for medical reasons (e.g., diabetic tracking).

Students who do not follow these rules will be sanctioned in the form of a temporary phone ban in the first instance or a permanent ban for persistent failure to follow these rules. In both these cases, the mobile phone is either left at home or can be handed in to reception for safe keeping in the morning and collected at the end of the school day.

School owned/provided devices:

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

Social media

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

School staff should ensure that:

- No reference should be made on social media to Church Stretton School, students, parents/carers, or school staff.
- They do not discuss personal matters about school community members online.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise the 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 it must not be linked in any way to Church Stretton School. Any such personal communications that are linked to Church Stretton School are within the scope of this policy and subject to the Disciplinary Procedure policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy, but still may be subject to the Disciplinary Procedure policy.
- Where personal use of social media in school outside of social time is suspected, and therefore interfering with relevant duties, disciplinary action may be taken.

Monitoring of public social media

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

Digital and video images

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

- When using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those Students whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *Students* in the digital/video image.
- *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.* As per the School's Code of Conduct, staff and volunteers should use School phones, tablets, video, and photography equipment to take images of pupils. School phones and cameras can be borrowed on request. All images of children should be stored securely and only accessed by those authorised to do so.
- *Students must not take, use, share, publish or distribute images of others without their permission.*
- *photographs published on the website, or elsewhere that include Students will be selected carefully and will comply with Online Safety Policy.*
- Written permission from parents or carers will be obtained before photographs of Students are taken for use in school or published on the school website/social media.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.
- Images will be securely stored in line with the school retention policy.
- *Students' work can only be published with the permission of the student and parents/carers.*

Online Publishing

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

- Public-facing website.
- Online newsletters.
- Email.

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

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

Data Protection

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

The school:

- Has a Data Protection Policy.
- Implements the data protection principles and can demonstrate that it does so.
- Has paid the appropriate fee to the Information Commissioner's Office (ICO)
- Has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- Has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where why and which member of staff has responsibility for managing it.
- The Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed.
- Has an 'information asset register' in place and knows exactly what personal data is held, where why and which member of staff has responsibility for managing it.
- Information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed.
- Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this.
- Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- Provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix).
- Has procedures in place to deal with the individual rights of the data subject, e.g., one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them.
- Carries out Data Protection Impact Assessments (DPIA) where necessary e.g., to ensure protection of personal data when accessed using any remote access solutions or entering a relationship with a new supplier.
- Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- Understands how to share data lawfully and safely with other relevant data controllers.
- Has clear and understood policies and routines for the deletion and disposal of data.

- Reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. To do this, it has a policy for reporting, logging, managing, investigating, and learning from information risk incidents.
- Has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- Provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

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

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

Staff must ensure that they:

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

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, Students; parents/carers and is reported to relevant groups:

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

Church Stretton School Online Safety Policy Appendices

Appendices

Appendix 1:

Student Acceptable Use Agreement Template

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal, and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students* to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the schools will monitor my use of the systems, devices, and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g., YouTube).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not use my own personal devices (mobile phones/USB devices etc.) in school. I understand that, if I do use my own devices in the school the device will be confiscated, and I will be subject to a phone ban.
- I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only not use social media sites in school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to act against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).

- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood, and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student Acceptable Use Agreement Form

This form relates to the student acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood, and agree to the rules included in the acceptable use agreement.

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school).
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g., communicating with other members of the school, accessing school email, website etc.

Name of Student:

Group/Class:

Signed:

Date:

Appendix 2:

Parent/Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should always have an entitlement to safe internet access.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people about their on-line behaviour.

The school will try to ensure that Students have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the student acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name:

Student Name:

Appendix 3:

Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people today, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should always have an entitlement to safe access to the internet and digital technologies.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that Students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g., laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g., on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Trust and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

Appendix 4:

Acceptable Use Agreement for Community Users Template

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices, and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices.

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: Signed: Date: .....

Appendix 5:

Policy for Harmful Sexual Behaviour

Statement of intent

Our school has a zero-tolerance approach to any harmful sexual behaviour involving children and acknowledge that it could be occurring at Church Stretton school and in our school community. The school is proactive in its approach to assessing prevalence, responding to incidents, and challenging and changing behaviour. This policy applies to all governors, staff, and students.

Schools and colleges have a statutory duty to safeguarding the children in their setting. We work together to foster an environment that creates healthy relationships for children and young people.

Our whole-school approach encourages healthy relationships and works to prevent harmful sexual behaviour. We provide high quality education within the curriculum to reduce the likelihood of the situations occurring.

We recognise that HSB (Harmful Sexual Behaviour) is harmful to both the child/children affected by the behaviours and the child/children who displayed the behaviour and provide ongoing support for all involved.

Our approach is to treat everything as safeguarding incident in the first instance - we distinguish between behaviours that are exploratory and part of healthy age and ability appropriate development and those that may be harmful.

As a school we provide regular opportunities for school staff to understand what harmful sexual behaviours might look like and what they should do in the event of a report.

Related policies

This policy should be read in conjunction with:

- Child protection and safeguarding policy
- Whistleblowing
- Behaviour policy
- Anti-bullying policy
- Online safety policy
- Acceptable Use Agreements

Definitions

As stated in the Sexual Offences Act 2003, the term Harmful Sexual Behaviour (HSB) covers a wide range of behaviours, often these may be considered problematic, abusive, or violent and may also be developmentally inappropriate. HSB can occur online, offline or in a blend of both environments. The term HSB is widely acknowledged in child protection and should be treated in this context.

Whilst peer on peer harassment has become a widely recognised term, this is already moving towards child on child in recognition that age and development is a factor in making decisions about behaviour. A significant age difference between the children involved in an incident may lead to a decision about the behaviour being harmful or not. For example, this could be an older child's behaviour towards a pre-pubescent child, or a younger child's behaviour towards an older child with learning difficulties. It is important that Designated Safeguarding Leads (DSL) know what is and is not HSB. DSLs (Designated Safeguarding Lead) should be involved in planning the curriculum for HSB, planning preventative actions, and ensuring a whole-schools culture that condones HSB, alongside all other forms of abuse and harassment. This template policy provides a basis for an effective approach to managing sexual violence and harassment.

What is sexual violence?

The following are sexual offences under the Sexual Offences Act 2003:

Rape: A person (A) commits an offence of rape if: he intentionally penetrates the vagina, anus, or mouth of another person (B) with his penis, B does not consent to the penetration and A does not believe that B consents.

Assault by Penetration: A person (A) commits an offence if: s/he intentionally penetrates the vagina or anus of another person (B) with a part of her/his body or anything else, the penetration is sexual, B does not consent to the penetration and A does not believe that B consents.

Sexual Assault: A person (A) commits an offence of sexual assault if: s/he intentionally touches another person (B), the touching is sexual, B does not consent to the touching and A does not believe that B consents. (NOTE- Schools and colleges should be aware that sexual assault covers a very wide range of behaviour so a single act of kissing someone without consent or touching someone's bottom/breasts/genitalia without consent, can still constitute sexual assault.)

Causing someone to engage in sexual activity without consent: A person (A) commits an offence if: s/he intentionally causes another person (B) to engage in an activity, the activity is sexual, B does not consent to engaging in the activity, and A does not believe that B consents.

(NOTE – this could include forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party.)

What is sexual harassment?

Keeping Children Safe in Education Guidance 2023 and the Sexual Violence and sexual harassment between children in schools and colleges state:

When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline and both inside and outside of school/college. When we reference sexual harassment, we do so in the context of child-on-child sexual harassment. Sexual harassment is likely to: violate a child's dignity, and/or make them feel intimidated, degraded, or humiliated and/or create a hostile, offensive or sexualised environment.

Whilst not intended to be an exhaustive list, sexual harassment can include:

- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance, and calling someone sexualised names.
- sexual "jokes" or taunting
- physical behaviour, such as: deliberately brushing against someone, interfering with someone's clothes (schools and colleges should be considering when any of this crosses a line into sexual violence – it is important to talk to and consider the experience of the victim) and displaying pictures, photos, or drawings of a sexual nature; and
- Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
- consensual and non-consensual sharing of nude and semi-nude images and/or videos. Taking and sharing nude photographs of U18s is a criminal offence.
    - sharing of unwanted explicit content
    - up skirting (this is a criminal offence)
    - sexualised online bullying.
    - unwanted sexual comments and messages, including, on social media.
    - sexual exploitation; coercion and threats.

It is important that schools and colleges consider sexual harassment in broad terms. Sexual harassment (as set out above) creates a culture that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence.

Responsibilities

Leaders and DSLs

Our leaders and DSLs have ultimate responsibility in dealing with all incidents of harmful sexual behaviour, including online. It is the expectation that all incidents of harmful sexual behaviour/sexual violence and harassment are reported in line with school safeguarding and child protection procedures.

We ensure that our designated safeguarding lead/s (DSL) and their deputies are confident in school safeguarding processes and when it is necessary to escalate. Our DSLs know what local and national specialist support is available to support all children involved in harmful sexual behaviour and are confident as to how to access this support when required.

Designated safeguarding lead/s and their deputies have an in-depth working knowledge of key documentation, particularly KCSIE (Keeping Children Safe in Education) 2022 and Sexual Violence and Sexual Harassment Between Children in Schools and Colleges (DfE 2021). We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

It is the role of school leaders and designated safeguarding leads to ensure that all staff and Governors receive training specific to harmful sexual behaviour, and that it is included as part of induction.

Staff

It is the responsibility of all staff to have read and understood this policy and associated policies. All staff must report any incidents or suspected incidents of harmful sexual behaviour to DSLs in line with school policy and ensure they are informed of the outcome. All staff will challenge any harmful sexual language or inappropriate behaviour. Staff have a duty to ensure that the school environment is one which is safe, and which supports Students to understand safe and healthy relationships and appropriate behaviour through delivery of our curriculum.

Governors

We ensure that our trust board/governing body have a good understanding of what harmful sexual behaviour is, when it can pose a risk to children and how to keep children safe. Our trustees/governors receive regular training and updates, both in terms of what sexualised behaviour is, but also how to effectively support establishments and their stakeholders whilst holding provision to account.

As part of the headteacher's report, our trust board/governing body has the opportunity to monitor and evaluate the approach to harmful sexual behaviour to ensure it is adequate and effective. This includes evaluation of the curriculum, pupil voice activity and evaluation of parent/carer engagement. Trustees/Governors ensure that risks relating to these issues are identified, that several reporting routes are available, and that risks are effectively mitigated.

Students

All Students have the right to learn in a safe, healthy, and respectful school environment. Our students benefit from a broad and balanced curriculum and are taught about healthy relationships and know how and when to report and that a range of different reporting routes is available to them. Our students are encouraged to report any harmful sexual behaviour, even if they are not directly involved. All Students will be believed if they make a disclosure and will be treated sensitively - whilst we cannot guarantee confidentiality, their thoughts and wishes will be considered when supporting them.

Parents/carers

We work hard to engage parents and carers by:

- regular in school sessions
- sharing newsletters
- sharing information online e.g., website, social media
- providing curriculum information
- List any other ways you may engage parents and carers e.g.

Our parents and carers are made aware of how and when to report any concerns to the school, that all incidents will be handled with care and sensitivity, and that it may sometimes be necessary to involve other agencies.

Vulnerable groups

We recognise that, nationally, vulnerable Students are three times more likely to be at risk from Harmful Sexual Behaviour. These include:

- A child with additional needs and disabilities.
- A child living with domestic abuse.
- A child who is at risk of/suffering significant harm.
- A child who is at risk of/or has been exploited or at risk of exploited (CRE, CSE (Child Sexual Exploitation)),
- A care experienced child.
- A child who goes missing or is missing education.
- Children who identify as, or are perceived as, LGBTQI+ and/or any of the other protected characteristics.

Children displaying HSB have often experienced their own abuse and trauma. We ensure that any vulnerable student is offered appropriate support, both within and outside school, sometimes via specialist agencies.

Reporting

Our systems are well promoted, easily understood and easily accessible for children and young people to confidently report abuse, knowing their concerns will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via:

- CPOMS for concerns about students
- Staff Safe for concerns about staff

Responding to an incident or disclosure

In this policy we recognise the importance of distinguishing between healthy, problematic, and sexually harmful behaviour (HSB)

Our response is always based on sound safeguarding principles and follows school safeguarding processes. It is calm, considered, and appropriate and puts the student at the centre of all decisions made.

List the school process if required.

The school will always adopt a multi-agency approach and seek external support and guidance, in line with school policy, if deemed necessary. This may include:

List relevant agencies e.g., MASH, Early Help, CAMHS, Police etc

Risk assessment

The school may deem it necessary to complete a harmful sexual behaviour risk assessment as part of the response to any reported incidents. The purpose of the risk assessment is the protect and support all those involved by identifying potential risk, both in and out of school (e.g., including public transport, after school clubs etc) and by clearly describing the strategies put in place to mitigate such risk.

The risk assessment will be completed following a meeting with all professionals working with the student, as well as parents or carers. Where appropriate, the students involved will also be asked to contribute.

The risk assessment will be shared will all staff who work with the student, as well as parents and carers. It will be dynamic and will respond to any changes in behaviour and will be regularly evaluated to assess impact.

Education

Our school's educational approach seeks to develop knowledge and understanding of healthy, problematic, and sexually harmful behaviours, and empowers young people to make healthy, informed decisions. Our school's approach is delivered through PSHE and RSE and additional opportunities are provided through:

- Cross curricular programmes (e.g., using the ProjectEVOLVE resources)
- Computing
- List other opportunities to deliver teaching and learning around HSB here e.g., assemblies, pastoral/form time, discrete lessons, visits from outside agencies etc.

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our setting. It is shaped and evaluated by Students and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this by:

- *Surveys*
- *Focus groups*
- *Parental engagement*
- *Staff consultation*
- *Staff training*

In line with good practice, we have created child-friendly versions of key safeguarding policies, produced, and regularly evaluated in consultation with young people. List those that are available below.

Training

It is effective safeguarding practice for the designated safeguarding lead (and their deputies) to have a good understanding of HSB. This could form part of their safeguarding training. This will aid in planning preventative education, implementing preventative measures, drafting, and implementing an effective child protection policy and incorporating the approach to sexual violence and sexual harassment into the whole school or college approach to safeguarding.

- Brook traffic light tool
- NSPCC training
- Whole staff training
- List other training the school has undertaken.

A clear training strategy which supports staff to respond effectively to different types of harassment and sexual misconduct incidents. This should involve an assessment of the training needs of all staff. This strategy should be reviewed and evaluated on a regular basis to ensure it is fit for purpose.

Training should be made available on an ongoing basis for all staff and students to raise awareness of harassment and sexual misconduct with the purpose of preventing incidents and encouraging reporting where they do occur.

Links

Child Exploitation and Online Protection command: CEOP is a law enforcement agency which aims to keep children and young people safe from sexual exploitation and abuse. Online sexual abuse can be reported on their website and a report made to one of its Child Protection Advisors

The NSPCC provides a helpline for professionals at 0808 800 5000 and help@nspcc.org.uk. The helpline provides expert advice and support for school and college staff and will be especially useful for the designated safeguarding lead (and their deputies)

Support from specialist sexual violence sector organisations such as Rape Crisis or The Survivors Trust

The Anti-Bullying Alliance has developed guidance for schools about Sexual and sexist bullying.

The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. The helpline provides expert advice and support for school and college staff regarding online safety issues

Internet Watch Foundation: If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF)

Childline/IWF Report Remove is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online

UKCIS Sharing nudes and semi-nudes advice: Advice for education settings working with children and young people on responding to reports of children sharing non-consensual nude and semi-nude images and/or videos (also known as sexting and youth produced sexual imagery).

Thinkuknow from NCA-CEOP provides support for the children's workforce, parents, and carers on staying safe online

Lucy Faithful Foundation

Marie Collins Foundation

NSPCC National Clinical and Assessment Service (NCATS)

Project deSHAME from Childnet provides useful research, advice, and resources regarding online sexual harassment.

Appendix 6: Record of reviewing devices/internet sites (responding to incidents of misuse)

Group:
Date:
Reason for investigation:

Details of first reviewing person
Name:
Position:
Signature:

Details of second reviewing person
Name:
Position:
Signature:

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Appendix 7: Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Appendix 8: Training Needs Audit Log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date