SPRINGHILL CATHOLIC PRIMARY SCHOOL

We strive to achieve excellence in all that we do as we follow the Gospel values of Jesus Christ.

Together we will do our best for Jesus

ONLINE SAFETY POLICY

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment

Adopted by the Governing Body: September 2024
Review Date: September 2026

Table of Contents

1. Context

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The staff and governors of Springhill recognise they have a duty to ensure that all pupils are able to make a valuable contribution to society and this is only possible to achieve if we ensure that pupils develop and apply their ICT capability effectively in their everyday lives.

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place, which are understood and adhered to by network users.

It is the duty of the school to ensure that every child in their care is safe, and the same principles apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties - the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements of school policy.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- Mobile phones
- Digital cameras
- e-mail
- Instant messaging
- Web cams
- Blogs/vlogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites

- Various apps
- Music download sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Smart Watches
- Tablets both android and Apple

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

• An effective range of technological tools;
• Policies and procedures, with clear roles and responsibilities;
• A comprehensive Online safety education programme for pupils, staff and parents.

2. Roles and Responsibilities

Online safety is recognized as a critical aspect of strategic leadership within this school. The Headteacher, with the support of the governing body, aims to embed safe practices into the school's culture. The Headteacher ensures the implementation of the policy and monitors compliance. Mrs. Ashworth has been designated the responsibility for online safety, and Miss Gallagher serves as the Computing Curriculum Leader.

Online Safety Coordinator and Computing Leader

Our Online Safety Coordinator stays up-to-date with online safety issues and guidance through liaison with the Local Authority Online Safety Officer and organizations such as WSGFL and the Child Exploitation and Online Protection (CEOP) Centre. They take day-to-day responsibility for online safety issues, provide training and advice for staff, and liaise with the school's network managers (AUX IT). The Online Safety Coordinator ensures that senior leadership, and the Full Governing Board (FGB) are updated as necessary. The Online Safety Coordinator:

- Takes day-to-day responsibility for online safety issues and plays a leading role in establishing and reviewing the school's online safety policies/documents;
- Ensures that all staff are aware of the procedures to follow in the event of an online safety incident;
- Provides training and advice for staff;
- Liaises with the Local Authority;
- Works with the school's technical staff;
- Receives reports of online safety incidents and logs them to inform future developments.

Headteacher/Designated Safeguarding Leads

- The Headteacher and other designated safeguarding leads are responsible for ensuring the safety of the school community, including online safety.
- They must be aware of the procedures to follow in the event of a serious online safety allegation against a staff member.
- They should be aware of procedures related to serious online safety allegations linked to the Prevent agenda and how to refer concerns to Channel.
- They ensure that all other staff receive appropriate training to enable them to carry out their online safety roles and train other colleagues as needed.
- They ensure that there is a system in place for monitoring and supporting those responsible for internal online safety monitoring roles, providing a safety net and support for colleagues in these roles**.**

Full Governing Board (FGB)

The FGB maintains an overview of online safety issues and strategies at the school. The Online Safety Coordinator will update the governing body at least once a year to ensure they are aware of changes in local and national guidance. A member of the FGB, Anita Tillyer has taken on the role of Online Safety Governor. The role includes:

- Regular meetings with the Online Safety Leader;
- Regular monitoring of online safety incident logs;
- Regular monitoring of filtering/change control logs;
- Reporting to the relevant Governors during meetings.

Teaching Staff and Support Staff

All teachers are responsible for:

- Promoting and supporting safe behaviours in their classrooms and following school online safety procedures.
- Ensuring that online safety is embedded in all aspects of the curriculum and other activities.

All staff are responsible for:

- Familiarizing themselves with the school's online safety policy and practices, including:
    - Safe use of email;
    - Safe use of the internet, including internet-based communication services such as instant messaging and social networking;
    - Safe use of the school network, equipment, and data;
    - Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
    - Publication of pupil information/photographs and the use of the website;
    - Procedures related to cyberbullying.
- Reading, understanding, and signing the Staff Acceptable Use Policy/Agreement (AUP);

- Reporting any misuse or problems to the Headteacher/Senior Leader for investigation/action;
- Monitoring the use of digital technologies, mobile devices, and cameras in lessons and other school activities, and implementing current policies;
- Guiding students/pupils to pre-checked sites in lessons where internet use is planned, and ensuring there are processes in place for dealing with unsuitable material found in internet searches.

Staff are reminded or updated about online safety matters at least once a year.

Designated Safeguarding Leads

The designated and deputy designated safeguarding leads should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data;
- Access to illegal/inappropriate materials;
- Inappropriate online contact with adults/strangers;
- Potential or actual incidents of grooming;
- Potential or actual incidents linked to radicalization;
- Cyberbullying.

IT Network Manager (AUX IT, Luke Prince)

The IT Network Manager is responsible for ensuring:

- The school's technical infrastructure is secure and not open to misuse or malicious attack;
- The school meets the required online technical requirements and any applicable Local Authority Online Policy/Guidance;
- Users can access the networks and devices only through a properly enforced password protection policy, with regular password changes;
- The filtering policy is applied and updated regularly, and that its implementation is not the sole responsibility of any one person (See Appendix D);
- They stay up-to-date with online technical information to effectively carry out their role and inform/update others as needed;
- Regular monitoring of the network/internet/remote access/email usage occurs to detect any misuse/attempted misuse, reporting these to the Headteacher/Senior Leader for investigation/action;
- Monitoring software/systems are implemented and updated as agreed in school policies.

Pupils

The school integrates online safety education within the Computing curricula. Every pupil is educated about safe and responsible online use, including how to control and minimize risks

and report problems. They are taught to keep passwords and personal information safe. Pupils are expected to:

- Use the school's digital technology systems in accordance with the Student/Pupil Acceptable Use Policy;
- Understand research skills, avoid plagiarism, and uphold copyright regulations;
- Report abuse, misuse, or access to inappropriate materials, and know how to do so;
- Know and understand policies on the use of mobile devices and digital cameras, including the use of images and cyberbullying;
- Adopt good online safety practices when using digital technologies outside of school, understanding that the school's Online Safety Policy covers their actions outside of school if related to their membership of the school.

Parents/Carers

The school actively engages with parents regarding online safety, providing education sessions yearly. The school helps parents understand how to educate their children on staying safe online through parents' evenings, newsletters, letters, and the school website. Parents and carers are encouraged to support the school by promoting good online practices and following guidelines on the appropriate use of:

- Digital and video images taken during school events;
- Conversations with their children at home about staying safe online.

Community Users

Community users who access school systems and websites as part of the wider school provision are required to sign a Community Users Acceptable Use Agreement (AUA) before being granted access.

3. Communications

How will the policy be introduced to pupils?

Many pupils are very familiar with the culture of new technologies, and have the main principles of this policy have been discussed with them. Pupils' perceptions of the risks are not always mature and hence; the online rules are explained or discussed in an age appropriate manner.

Online education is currently placed within our Online Safety Curriculum Map. We use Project Evolve resources and the PSHE Association scheme in PDL to support and structure the teaching. We also integrate online teaching within the curriculum for Computing. Each year group has a set of online objectives which children are taught in computing lessons.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. Staff are given opportunities to discuss the issues and develop appropriate teaching strategies

Staff understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and induction of new staff includes a discussion of the school's Online Safety Policy.

• Staff are aware that internet traffic is monitored and can be traced to the individual user.
• Discretion and professional conduct is essential.
• Staff that manage filtering systems or monitor ICT use are supervised by Senior Leaders and have clear procedures for reporting issues.
• Staff training in safe and responsible Internet use and on the school Online Safety Policy is provided as required.

How will parents' support be enlisted?

Internet use in pupils' homes is an everyday activity. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school is able to help parents plan appropriate supervised use of the internet at home by:
• Encouraging a partnership approach which includes:
    - Providing a designated online area on our website giving advice on filtering systems and educational and leisure activities that include responsible use of the Internet for parents.
    - Providing references to relevant websites/publications e.g. www.safertinternet.org.uk, http://childnet.com/parents-and-carers, and https://www.thinkuknow.co.uk.
• Ensuring that Internet issues will be handled sensitively, and parents will be advised accordingly.

How will complaints regarding online safety be handled?

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

• interview by theHeadteacher/DSL;
• informing parents or carers;
•removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];

• referral to the Police.

Our safeguarding leads acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
Complaints related to child protection are dealt with in accordance with school /child protection procedures.

4. Managing the Internet Safely

The risks:

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse.

Technical and Infrastructure:

The school has a managed ICT service provided by an outside contractor (AUX IT), but it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school. It is important that the managed service provider is fully aware of the school's Online Safety Policy/Acceptable Use Agreements.

This school:
• Maintains the filtered broadband connectivity through Exa networks;
• Ensures their network is 'healthy' by having health checks annually on the network;
• Utilises caching as part of the network set-up;
• Ensures the Systems Administrator / network manager is up-to-date with WSGfL services and policies;
• Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
• Never allows pupils access to Internet logs;
• Never sends personal data over the Internet unless it is encrypted or otherwise secured;
• Never allows personal level data off-site unless it is on an encrypted device;

• Uses 'safer' search engines with pupils where appropriate, e.g. Kiddle;

Policy and Procedures:

This school:

• Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
• We use the Exa Networks SurfProtect filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature (see Appendix D);
• Uses Senso software to monitor pupils' and staff's use of the internet and software on the computers. Real time alerts are sent to Miss Gallagher and Mrs Ashworth as they happen and a weekly report of infringements and misuse is sent to the Head Teacher.
• Staff preview all sites before use, where not previously viewed and cached.
• Plans the curriculum context for Internet use to match pupils' ability, using child friendly search engines where more open internet searching is required;
• Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
• Informs users that Internet use is monitored;
• Informs staff and pupils that that they must report any failure of the filtering systems directly to the IT Network Manager (AUX IT).
• Only uses approved or checked webcam sites;
• Keeps a record, e.g. CPOMS, of any online bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
• Ensures the named child protection officer has appropriate training;
• Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
• Immediately refers any material we suspect is illegal to the appropriate authorities, including the Police and the Local Authority.

Education and training:

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Reinforces key online safety messages in a planned programme of assemblies and class activities;
- Ensures that students understand the need for the Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school;

- Has a clear, progressive online safety education programme throughout the curriculum all Key Stages, built on Hampshire / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as: to STOP and THINK before they CLICK;
- to discriminate between fact, fiction and opinion;
- to develop a range of strategies to validate and verify information before accepting its accuracy;
- to skim and scan information;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know some search engines / web sites that are more likely to bring effective
- results; to know how to narrow down or refine a search;
- to understand how search engines work;
- to understand 'Netiquette' behaviour when using an online environment / email,
- i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files - such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;

Copyright and Plagiarism:

This school:

• Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
• Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on- line; on-line gaming / gambling;
• Ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities;
• Makes training available to staff on the online education program;
• Runs a rolling programme of advice, guidance and training for parents, including:
  - information in school newsletters and on the school web site;
  - demonstrations, practical sessions held at school;
  - suggestions for safe Internet use at home;

- provision of information about national support sites for parents.

5. Managing e-mail

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes.

This school:
• Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for any communication with the wider public;
• All parent/carer emails are received at a central email address for screening (info@springhillcatholic.net)
• Contacts the police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law;
• Manages accounts effectively, with up to date account details of users;
• Reports messages relating to or in support of illegal activities;
• Staff use Office 365 e-mail systems for professional purposes.

6. Use of Digital and Video images

In this school:
• The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
• Uploading of information is restricted to the website team;
• The school web site complies with the school's statutory requirements;
• The point of contact on the website is the school address and telephone number. Home information or individual e-mail identities are not published;
• Photographs published on the web, Xor Facebook do not have names attached;
• We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
• Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year - unless an item is specifically kept for a key school publication;
• We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
• We do not include the names of pupils in the credits of any published school produced video materials / DVDs;
• Pupils are taught about how images can be abused in computing lessons.

7. Social Media – Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes, a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when

publishing any material online. Expectations for teachers' professional conduct are set out in
'Teachers Standards 2012, while Ofsted's Online Safety framework 2012 reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information in the staff code of conduct.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

8. Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:
• Fairly and lawfully processed;
• Processed for limited purposes;
• Adequate, relevant and not excessive;
• Accurate;
• Kept no longer than is necessary;
• Processed in accordance with the data subject's rights;
• Secure;
• Only transferred to others with adequate protection.

The school must ensure that:
• It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
• Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
• All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". Please see the Freedom of Information publication hosted on the school's website;
• It has a Data Protection Policy;
• It is registered as a Data Controller for the purposes of the Data Protection Act (DPA);
• Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs);
• Risk assessments on IT are carried out and are kept up to date;
• It has clear and understood arrangements for the security, storage and transfer of personal data;
• Data subjects have rights of access and there are clear procedures for this to be obtained;
• There are clear and understood policies and routines for the deletion and disposal of data

• There is a policy for reporting, logging, managing and recovering from information risk incidents;
• There are clear Data Protection clauses in all contracts where personal data may be passed to third parties;
• There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:
• At all times, take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse;
• 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 and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:
• The data must be password protected;
• The device must be password protected;
• The device must offer approved virus and malware checking software;
• The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
Data is never stored on a memory stick that is not password protected.

9. Managing equipment

The computer system / network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely this school:

• Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
• Makes clear that pupils should never be allowed to log-on or use teacher and staff logins - these have far less security restrictions and inappropriate use could damage files or the network;
• Makes clear that no one should log on as another user - if two people log on at the same time this may corrupt personal files and profiles;
• Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;

• Requires all users to always log off when they have finished working or are leaving the computer unattended. Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
• Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed;
• Maintains equipment to ensure Health and Safety is followed;
• Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
• Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
• Follows local authority advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
• Reviews the school ICT systems regularly with regard to security.

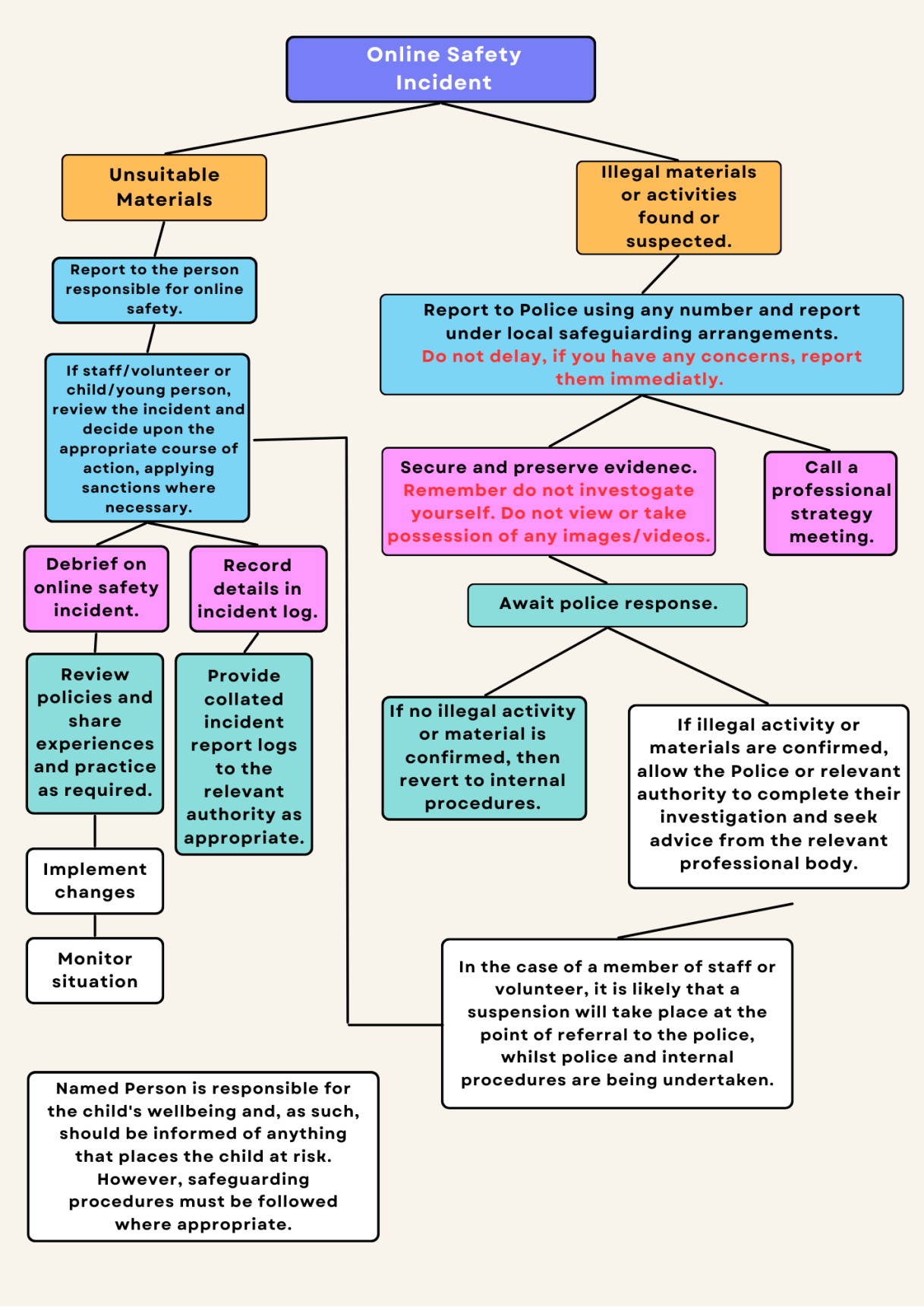
10. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities and the appropriate action must be taken and recorded.

10.1 Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or is there is any other suspected illegal activity, refer to the right hand side of the flowchart for responding to online safety incidents and report immediately to the police.

Appendix A: Online Safety Flowchart.



10.2 Other Incidents

It is hoped that all members of the school community, who understand and follow the school policy, will be responsible users of digital technology. However, there may be times when infringements of the policy could take place, through careless, irresponsible or deliberate misuse.

Whenever a student or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the school management. These sanctions can be found in Appendix C – Handling of Infringements.

In the event of suspicion, all steps in this procedure should be followed:

• Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

• Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

• It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse – see below).

• Once this has been completed and fully investigated the designated group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action.

• If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour;
- The sending of obscene materials to a child;
- Adult material which potentially breaches the Obscene Publications Act;
- Criminally racist material;
- Other criminal conduct, activity or materials.

• 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 of 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.

1.3 Incidents outside of school

If any incidents occur outside of school then the parents are responsible for dealing with it. If the school is made aware of any incidents, then as a school we will, depending on the severity, refer to the handling of infringements process in Appendix C. We will treat each incident on an individual basis, and work closely with the parents to decide on what action should be taken.

11. Cyber-bullying

11.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

11.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. [Class teachers/form teachers] will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

11.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

Poses a risk to staff or pupils, and/or

Is identified in the school rules as a banned item for which a search can be carried out, and/or

Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from [the headteacher / DSL / appropriate staff member]

Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

Cause harm, and/or

Undermine the safe environment of the school or disrupt teaching, and/or

Commit an offence

If inappropriate material is found on the device, it is up to [the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team] to decide on a suitable response. If there are images, data or files on the device that staff reasonably

suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

Not view the image

Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision

Any searching of pupils will be carried out in line with: The DfE's latest guidance on searching, screening and confiscation UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Our behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

11.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

[School or trust name] recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

[School or trust name] will treat any use of AI to bully pupils in line with our [anti-bullying/behaviour] policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust

12. Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of:
- Senior Leaders;
- Online Safety Leader and Computing Leader;
- Staff – including Teachers, Support Staff and Technical staff;
- Governors;
- Parents/Carers

Schedule

Online Safety Policy approved by the FGB. Annually - June
The implementation of this Online Safety policy will be monitored by the:

Computing Leader and the Senior Leadership Team
Monitoring will take place as alerts arise.
The Governing Board will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of the Online Safety Incidents) at regular intervals:
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:

September 2025

The school will monitor the impact of this policy using:
- Logs of reported incidents;
- Monitoring logs of internet activity (including sites visited);
- Internal monitoring data for network activity;

Appendix B:
School Technical Security Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:
- Users can only access data to which they have right of access;
- No user can access another's files (other than that allowed for monitoring purposes within the school's policies);

• Access to personal data is securely controlled in line with the school's personal data policy;
• Logs are maintained of access by users and of their actions while users of the system;
• There is effective guidance and training for users;
• There are regular reviews and audits of the safety and security of school computer systems;
• There is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the school's IT Network Manager.

Technical Security

The school will be 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. It will also ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:
• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements;
• There will be regular reviews and audits of the safety and security of school technical systems;
• Servers, wireless systems and cabling will be securely located and physical access restricted;
• Appropriate security measures will be in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data;
• All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the IT Network Manager and will be reviewed, at least annually, by the Online Safety Group;
• Users will be responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
• The IT Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs;
• Mobile device security and management procedures are in place to ensure that the tablets and laptops are secured on the school's network through the chosen system;
• Never allowing friends/family use school devices.
• An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system;
• An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users;

• The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc;
• Personal data cannot be sent over the internet or taken off the school site, unless passworded or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices and email.

Policy Statements

• All users will 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 Network Manager and will be reviewed, at least annually, by the Online Safety Lead.
• All school networks and systems will be protected by secure passwords that are regularly changed. Consideration should also be given to using two factor authentication for such accounts.
• Passwords for new users, and replacement passwords for existing users will be allocated by the school's IT Network Manager.
•All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
• Users will change their passwords at regular intervals – as described in the staff and student /pupil sections below.
• The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account.

Staff passwords:

• All staff users will be provided with a username and password by the school's IT Network Manager who will keep an up to date record of users and their usernames.
• The password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters.
• Must not include proper names or any other personal information about the user that might be known by others.
• The account should be "locked out" following six successive incorrect log-on attempts.
• Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
• Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
• Should be changed at least every year.
• Should not re-used for 6 months and be significantly different from previous password. The last four passwords cannot be re-used passwords created by the same user.
• Should be different for systems used inside and outside of school

Student / pupil passwords

• Students / pupils will be taught the importance of password security through the Computing curriculum.
• Pupils in Year 1 will receive their log ins which they will use until the end of year 6.

Pupils / students will be made aware of the school's password policy:
• in lessons through the Computing Online Safety curriculum;
• through the Acceptable Use Agreement.

Audit / Monitoring / Reporting / Review

The responsible person, IT Network Manager, will ensure that full records are kept of:
• User Ids and requests for password changes;
• User log-ons;
• Security incidents related to this policy.

Appendix C:
Handling of infringements

Pupils

Category A infringements
• Use of non-educational sites during lessons
• Unauthorised use of email
• Use of unauthorised instant messaging / social networking sites.

Category A sanctions
• Referral to class teacher or member of the SLT or reflection time.

Category B infringements
• Continued use of non-educational sites during lessons after being warned;
• Continued unauthorised use of email after being warned;
• Continued use of unauthorised instant messaging / chat rooms, social networking sites, Newsgroups;
• Accidentally accessing offensive material and not logging off or notifying a member of staff of it.

Category B sanctions
• Referral to Headteacher or Senior Assistant Headteacher;
• Removal of Internet access rights for a period;
• Raise CPOMS;
• Contact with parent.

Category C infringements
• Deliberately corrupting or destroying someone's data, violating privacy of others;
• Sending an email or message that is regarded as harassment or of a bullying nature (One-off);
• Deliberately trying to access offensive or pornographic material;
• Any purchasing or ordering of items over the Internet;
• Transmission of commercial or advertising material.

Category C sanctions
• Referral to Headteacher or Deputy Headteacher;
• Removal of internet rights for a more extended period;

• Contact with parents;
• Raise CPOMS.

Other safeguarding actions:

If inappropriate web material is accessed:
1. Ensure appropriate technical support filters the site
2. Referral to Headteacher or Lead Assistant Headteacher.

Category D infringements
• Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned;
• Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
• Bringing the school name into disrepute.

Category D sanctions
• Referred to Headteacher;
• Contact with parents;
• Possible exclusion;
• Refer to Community Police Officer;
• Local Authority Online officer;
• Raise CPOMS.

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
• Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
• Not implementing appropriate safeguarding procedures.
• Any behaviour on the World Wide Web that compromises the staff members' professional standing in the school and community.
• Misuse of first level data security, e.g. wrongful use of passwords.
• Breaching copyright or license e.g. installing unlicensed software on network.

Category B infringements (Gross Misconduct)
• Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
• Any deliberate attempt to breach data protection or computer security rules;
• Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
• Bringing the school name into disrepute.

[Sanction - Referred to Headteacher / FGB and follow school disciplinary procedures; Discuss with HR advisor, report to Police]

Other safeguarding actions:
• Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
• Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
• Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that, the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Human Resources Advisor.

Child Pornography
In the case of Child Pornography being found, the member of staff should be immediately suspended and the Police should be called. Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP).

How will staff and pupils be informed of these procedures?

• They are fully explained and included within the school's Online / Acceptable Use Policy. All staff will be required to sign the school's Acceptable Use Policy.
• Pupils are taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate acceptable use form.
• The school's online policy is made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
• Information on reporting abuse / bullying etc. is made available by the school for pupils, staff and parents.

Appendix D:
Filtering
Introduction
The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for Online Safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities
The responsibility for the management of the school's filtering policy will be held by the school's Network Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to the school's Network Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering /security systems in place to prevent access to such materials.

Policy Statements
Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.
• The school maintains and supports the managed filtering service provided by

SurfProtect.

• The school has provided enhanced / differentiated user-level filtering through the use of the SurfProtect filtering programme, allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.

•In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).

• Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems

• Any filtering issues should be reported immediately to the filtering provider.

• The use of Senso software supports the monitoring of the online behaviour and sends notification to the Network Manager, Computing Subject Leader and the Headteacher.

• Requests from staff for sites to be removed from the filtered list will be considered by the school's Network Manager and Computing Leader. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

• The Acceptable Use Agreement;

• Induction training;

• Staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through Online Safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the school's Network Manager and the Computing Leader who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

• The second responsible person, the Computing Leader

• Online Safety Governor

• External Filtering provider / Local Authority / Police on request.

Appendix E:
KS2 Acceptable Use Policy

These statements can keep me and others safe & happy at school and home

1. ***I learn online*** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.
5. ***I am a good friend online*** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am not a bully*** – I know just calling something fun or banter doesn't stop it maybe hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
11. ***If I make a mistake I don't try to hide it but ask for help.***
12. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
13. ***I know online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
14. ***I never pretend to be someone else online*** – it can be upsetting or even dangerous.
15. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
16. ***I don't go live (videos anyone can see) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
17. ***I don't take photos or videos or people without them knowing or agreeing to it*** – and I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.

18. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
19. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
20. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
21. ***I follow age rules*** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
22. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
23. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
24. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
25. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
26. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
27. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, and I know which sites to trust, and how to double check information I come across. If I am not sure I ask a trusted adult.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult

Appendix F:
EYFS/KS1 Acceptable Use Policy:

To stay **SAFE online and on my devices**, I follow the Digital 5 A Day and:

1. I only **USE** devices or apps, sites or games if I am allowed to
2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused
3. I look out for my **FRIENDS** and tell someone if they need help
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I **KNOW** that online people aren't always who they say they are and things I read are not always **TRUE.**
6. Anything I do online can be shared and might stay online **FOREVER**
7. I don't keep **SECRETS** 🚫 unless they are a present or nice surprise
8. I don't have to do **DARES OR CHALLENGES** ❌, even if someone tells me I must.
9. I don't change **CLOTHES** or get undressed in front of a camera
10. I always check before **SHARING** my personal information or other people's stories and photos
11. I am **KIND** and polite to everyone

Appendix G:
Staff Member / Governor / Volunteer / Visitor Acceptable Use Policy

The computer system is owned by the school and is made available to staff to enhance their professional activities, including teaching, research, administration, and management. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited. All staff (including supply and temporary) requiring internet access should sign a copy of this Acceptable Use Statement.

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device:

- I will make sure that any issued devices are used only by staff.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will not share confidential information about the school, its pupils, staff, or other members of the community.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal details, such as mobile phone numbers and personal email addresses, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will only open email attachments from sources I know to be safe.
- I will not install any unauthorised software, or connect unauthorised hardware or devices to the school's network.
- I will ensure that personal data (such as data held on SIMS and CPOMs) is kept secure and is used appropriately, whether in school, taken off the school premises, or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
- I will not access, or attempt to access, inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (nor will I create, share, link to, or send such material).
- I will ensure that images of pupils and/or staff will only be taken and stored on school devices. Photos will be deleted from iPads after use. Photos of children should only be taken with written consent from the parent/carer. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff, or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will not access the school's wireless internet on personal mobile devices.
- I will use the same professional levels of language and content as for letters or other media.
- I will make sure no reference is made to Springhill Primary School on any social networking site.
- I will support and promote the school's Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I understand that:

- The school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will inform the designated safeguarding lead (DSL) if a pupil informs me they have found any material which might upset, distress, or harm them or others. I will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.