SNARESBROOK PREPARATORY SCHOOL

E-Safety (including Online Activities)

[Policy #020]

This policy relates to the whole school, including Early Years Foundation Stage (EYFS) and all activities, including residential trips and all care arrangements.

Linked Policies:

- 001 Child Protection / Safeguarding
- 081 Sexual Violence and Sexual Harrassment Policy.

This policy has regard to:

- Keeping Children Safe in Education September 2025 - Statutory guidance for schools and colleges on safeguarding children and safer recruitment.
- Relationship Education, Relationships and Sex Education and Health Education Statutory Guidance
- Teaching Online Safety in Schools June 2019 (DfE Advice)
- Education for a Connected World
- National curriculum in England: computing programmes of study - Statutory guidance on computing programmes of study.
- How Social Media is Used to Encourage Travel to Syria and Iraq
- Cyber-bullying: Advice for headteachers and school staff (2014) and Advice for parents and carers on cyber-bullying (2014).
- Relationship Education (primary) (2021)
- Meeting Digital and Technology Standards in School

Approved by:	Head	**Last reviewed by:**	Head
Date last approved:	30-Nov-2024	**Date last reviewed:**	30-Nov-2024
Next approval due:	1 year from above date	**Next review due:**	1 year from above date

Contents (hyperlinks)

page

1 Policy Statement

1.1 The school will adopt a zero tolerance approach to any cyber bullying issues. All staff will challenge any abusive behaviour between peers that comes to their notice and will report on to the DSL immediately any issues of this nature. Please see Safeguarding policy for further details about dealing with child-on-child abuse or/as well as the Sexual Violence and Sexual Harrassment Policy.

1.2 Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. We equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

1.3 It is essential that children are safeguarded from potentially harmful and inappropriate online material. Our effective whole school approach to online safety empowers us to protect and educate our pupils, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

1.4 The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

1.4.1 **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

1.4.2 **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.

1.4.3 **conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

1.4.4 **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, or staff/colleagues are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

1.5 Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a

whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

1.5.1 Websites;

1.5.2 Learning platforms and virtual learning environments;

1.5.3 Email and Internet messaging;

1.5.4 Chat rooms and social networking;

1.5.5 Social Media, Blogs and wikis;

1.5.6 Podcasting;

1.5.7 Video broadcasting inc. Vlogging ;

1.5.8 Music downloading;

1.5.9 Gaming;

1.5.10 Mobile/smart phones with text, video and or web functionality;

1.5.11 Other mobile devices with web functionality.

1.6 Whilst exciting and beneficial both in and out of the context of education, much of ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

1.7 At SPS we understand the responsibility to educate our pupils in e-Safety issues; teaching them to remain safe and legal when using the Internet and related technologies, in and beyond the context of the classroom. As such we embed teaching about online safety and harms within a whole school approach that includes:

1.7.1 Creating a culture that incorporates the principles of online safety across all elements of school life;

1.7.2 Proactively engaging staff, pupils and parents/carers;

1.7.3 Reviewing and maintaining the online safety principles and systems;

1.7.4 Embedding the online safety principles and systems;

1.7.5 Modelling the online safety principles consistently.

2 Roles and responsibilities

2.1 As e-Safety is an important aspect of strategic leadership within the school, the Head and board of directors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

2.2 The board will always ensure a member of SLT will take the lead on e-safety in the school and are overseen by a member of the board. Currently this is the Designated Safeguarding Governor.

2.3 The DSL (P Raj) takes the lead responsibility for e-safety and filtering and monitoring in the school. All members of the school community have been made aware of who holds the post. It is the role of the DSL is to keep abreast of current issues and guidance. The DSL updates senior management and directors and all directors have an understanding of the issues at our school in relation to local and national guidelines and advice.

2.4 The designated safeguarding lead/ (DDSL) should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This is explicit in the role holder's job description.

2.5 The SLT member is responsible for:

- 2.5.1 buying filtering and monitoring systems
- 2.5.2 documenting decisions on what is blocked or allowed and why
- 2.5.3 reviewing the effectiveness of your provision
- 2.5.4 overseeing reports

2.6 They are also responsible for making sure that all staff:

- 2.6.1 understand their role
- 2.6.2 are appropriately trained
- 2.6.3 follow policies, processes and procedures
- 2.6.4 act on reports and concerns

2.7 The DSL is responsible for:

- 2.7.1 checking relevant reports
- 2.7.2 responding to safeguarding concerns identified by filtering and monitoring
- 2.7.3 providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly

2.7.4 taking any necessary action in line with Keeping children safe in education and your existing safeguarding policies.

2.7.5 Making sure all users, parents and carers are aware of your policy.

2.7.6

2.8 The compliance sub-committee, chaired by the Safeguarding Director, annually reviews the effectiveness of school filters and monitoring systems and ensures that the leadership team and relevant staff are aware of and understand the systems in place, manage them effectively and know how to escalate concerns when identified.

2.9 It is everyone's responsibility to monitor pupils' use of the internet and technology to keep them safe. The analogy is that the school's filters are like the school walls or fence, and the monitoring is what we do when they are in our care; for example, when it is break time. Whenever IT is being used that can access the internet, members of staff should be able to see the screen as often as possible. This might require members of staff to position themselves behind the students and they should avoid setting up laptops, ipads, etc. in a way or in a space that makes it hard for staff to monitor at a distance. Staff are regularly trained in their responsibilities for filtering and monitoring at staff meetings.

2.10 Day-to-day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT support to be effective. The board will ensure that the person with day-to-day responsibility is appropriately trained and works with the DSL. Currently the day-to-day duties are the responsibility of the IT Manager.

2.11 The IT Manager is responsible for:

2.11.1 maintaining filtering and monitoring systems
2.11.2 providing filtering and monitoring reports
2.11.3 completing actions following concerns or system checks
2.11.4 working with the SLT and DSL to:
2.11.4.1 help buy systems
2.11.4.2 identify risk
2.11.4.3 carry out reviews
2.11.4.4 carry out checks

3 The Scope of this policy

3.1 This policy covers the following areas of E-Safety:

3.1.1 Teaching and Learning;

3.1.2 E-Safety skills development for staff;

3.1.3 E-Safety information for parents/carers;

3.1.4 Managing Internet Access;

3.1.5 Email Access;

3.1.6 Published content and the school website;

3.1.7 Publishing pupil's images and work;

3.1.8 Photographs taken by parents/carers for personal use;

3.1.9 Social networking and personal publishing;

3.1.10 Managing filtering;

3.1.11 Protecting personal data;

3.1.12 Authorising Internet access;

3.1.13 Password security;

3.1.14 Assessing risks;

3.1.15 Handling e-Safety complaints;

3.1.16 Communications policy;

3.1.17 Introducing the e-Safety policy to pupils;

3.1.18 Staff and the e-Safety Policy;

3.1.19 Monitoring and review.

4 Writing and reviewing the e-Safety policy

4.1 This policy, supported by the school's Acceptable User Agreement for staff, directors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to our policies covering ICT (home school agreements) Behaviour, Bullying, Health & Safety, Safeguarding (inc Radicalisation, Extremism and Terrorism) and PSHE.

4.2 Our e-Safety policy has been written by the school in conjunction with: advice about online safeguarding trends from our local authority,Redbridge; the Independent Schools Association; and government guidance. It has been agreed

by the leadership team, communicated to staff and approved by the board of directors. The e-Safety policy and its implementation will be reviewed annually.

5 Handling e-Safety complaints

5.1 Complaints of Internet misuse will be dealt with by the e-Safety Coordinator.

5.2 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety Coordinator and recorded in the e-Safety incident logbook.

5.3 Any complaint about staff misuse must be referred to the Headteacher.

5.4 Complaints of a safeguarding nature including radicalisation, extremism and terrorism must be dealt with in accordance with school's safeguarding procedures and the Prevent Duty.

5.5 Pupils and parents will be informed of the complaints procedure.

6 Introducing the e-Safety policy to pupils

6.1 E-safety rules will be discussed with the pupils throughout the year. Specific lessons will be taught by class teachers at relevant points throughout e.g. during PSHE lessons/circle times/anti bullying discussions.

6.2 Pupils will be informed that network and Internet use will be monitored.

7 Staff and the e-Safety Policy

7.1 All staff will be given the school e-Safety policy and its importance will be explained.

7.2 Any information downloaded must be respectful of copyright, property rights and privacy.

7.3 Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.

7.4 A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software both in and out of school.

7.5 Regular random checks are made on the network which includes radicalisation and extremism filters. Under the Prevent Duty 2015, any issues of this nature will be initially handled by the e-Safety coordinator and then passed to the DSL for action.

7.6 Monitoring and Review

7.7 This section has reference to the Government's guidance which can be found here.

7.8 The policy is implemented on a day to day basis by all school staff and is monitored by the IT Manager.

7.9 The policy is the Director's responsibility and they will review its effectiveness annually.

7.10 The proprietor has overall strategic responsibility for meeting this standard. They will make sure that filtering and monitoring provision is reviewed at least once every academic year.

7.11 The review will be conducted by members of the senior leadership team, the designated safeguarding lead, and IT support. It will also involve the Safeguarding Director. The results of the online safety review will be recorded on this form and made available to anyone who is entitled to inspect that information.

7.12 A review of filtering and monitoring should be carried out to identify the current provision, any gaps, and your students' and staff's specific needs.

7.13 The aim of the review is to understand:

- 7.13.1 pupils' risk profile
- 7.13.2 How this informs the leaders' approach to filtering and monitoring considering things such as their:
  - 7.13.2.1 age,
  - 7.13.2.2 if they have any special education needs and disabilities (SEND) and
  - 7.13.2.3 whether they have English as an additional language (EAL)
- 7.13.3 what the filtering system currently blocks or allows
- 7.13.4 technical limitations, for example, whether the solution can filter real time content

7.13.5 any outside, contextual, or specific safeguarding influences,

7.13.6 any relevant safeguarding reports or serious incidents

7.13.7 the digital resilience of your students

7.13.8 teaching requirements, for example, your relationships, sex and health education (RHSE) and personal, social, health and economic (PSHE) curriculum

7.13.9 The school's current uses technology, including any bring your own device (BYOD), and generative AI tools

7.13.10 what related safeguarding or technology policies are in place

7.13.11 what checks are currently taking place and how resulting actions are handled

7.13.12 any technical set-up recommendations to make sure the system works effectively

7.14 To make your filtering and monitoring provision effective, the review will inform:

7.14.1 The related safeguarding and technology policies and procedures

7.14.2 roles and responsibilities of the Safeguarding Director, DSL, SLT, IT Manager, wider staff, parents and pupils

7.14.3 staff training

7.14.4 curriculum and learning opportunities

7.14.5 how often and what is checked

7.14.6 monitoring strategies

7.14.7 procurement decisions

7.15 Following system or equipment changes, the Safeguarding Director will seek assurance that all filtering and monitoring solutions will continue to work on all school-managed devices.

7.16 The review should take place, as a minimum, once every academic year or when:

7.16.1 a safeguarding risk is identified

7.16.2 there is a change in working practice, like remote access or BYOD

7.16.3 new technology is introduced, such as new devices

7.16.4 major software updates occur

7.17 there are changes to the technical configuration of the network and devices

7.18 If the review identifies any risks or issues with filtering and monitoring on devices, the IT manager will investigate and will resolve the issue by reviewing the filtering and monitoring provision or adjusting the device settings.

7.19 Consideration will be given to our pupils' risk profile when deciding whether to continue using the devices in question.

7.20 Checks to your filtering provision need to be completed and recorded as part of your filtering and monitoring review process. Checks should be made from both a safeguarding and IT perspective.The IT manager checks the logs daily and the DSL reviews these at least weekly.

7.21 Once a term the IT manager will check the following:

7.21.1 school owned devices and services – including laptops, tablets and audiovisual equipment, whether used at home or at school

7.21.2 All locations - main building, EYFS building, and Hall.

7.21.3 that user group accounts are filtering the correct content for pupils, staff and guests

7.22 The IT manager will keep a log of your checks so they can be reviewed. The log will record:

7.22.1 when the check took place

7.22.2 who did the check

7.22.3 what they tested or checked

7.22.4 resulting actions

7.22.5 Results from South West Grid for Learning's (SWGfL) testing tool to check that, as a minimum, the filtering system is blocking access to:

7.22.5.1 illegal child abuse material

7.22.5.2 unlawful terrorist content

7.22.5.3 adult content

7.22.6 That blocklists included with the filtering solutions cover lists provided by The Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU)

7.22.7 That the filtering provider is:

7.22.7.1 a member of IWF

7.22.7.2 signed up to CTIRU

7.22.7.3 regularly updates blocklists based on information from IWF and CTIRU

7.22.8 That any additions to the blocklist not disrupt or affect teaching and learning.

7.22.9 the filtering system is active, up to date and applied to all:

7.22.9.1 school or college-managed devices, including those taken off-site

7.22.9.2 unmanaged devices under a bring your own device (BYOD) scheme

7.22.9.3 guests who have access to the school internet

7.22.10 Devices that are not school or college-managed are on a separate virtual network.

7.22.11 Technical monitoring systems being used notify users that the device is being monitored. This could be a message each time they log in.

7.22.12 the filtering system:

7.22.12.1 identifies and appropriately filters all internet feeds, including any backup connections and portable wifi devices

7.22.12.2 is appropriate for the age and ability of the users

7.22.12.3 is suitable for educational settings

7.22.12.4 identifies multilingual web content, images, common misspellings and abbreviations

7.22.12.5 provides alerts when web content of concern has been blocked

7.22.12.6 blocks technologies and techniques that allow users to get around the filtering, such as VPNs, proxy services and end-to-end encryption methods

7.22.12.7 confirmation from the filtering provider as to whether it can provide filtering on mobile or app technologies.

7.22.12.8 allows the school to identify:

7.22.12.8.1 device name or ID,

7.22.12.8.2 IP address, and

7.22.12.8.3 where possible, the individual

7.22.12.8.4 the time and date of attempted access

7.22.12.8.5 the search term or content being blocked

7.22.13 That all search engines have safe search enabled by default, or use a child-friendly search engine,

7.22.14 your safe search engine is locked into your chosen browser and cannot be changed

7.22.15 users cannot download additional browsers or unauthorised plugins

7.22.16 If the filtering provision is procured with a broadband service, evidence from the broadband provider as to how it meets these requirements.

7.22.17 monitoring systems are working as expected both on-site and off-site

7.22.18 provide reporting on student device activity

7.22.19 That the person/people responsible for system based monitoring receive safeguarding training including online safety

7.22.20 That the person/people responsible for system based monitoring record and report safeguarding concerns to the DSL

7.22.21 That monitoring data:

7.22.22 is received in a format that staff can understand

7.22.23 Ensures users are identifiable, so concerns can be traced back to an individual, including guest accounts

7.22.24 That where mobile or app technologies are used technical monitoring systems are applied to the devices,

7.22.25 That the monitoring systems have regard to, would identify and alert the IT Manager to the 4 areas of risk and associated behaviours that users may experience when online as outlined in KCSIE.

7.22.26 Technical monitoring systems do not stop unsafe activities on a device or online.

7.23 The DSL will ensure that all staff are aware of reporting mechanisms for safeguarding and technical concerns and they should report if:

7.23.1 they witness or suspect unsuitable material has been accessed

7.23.2 they can access unsuitable material

7.23.3 they are teaching topics which could create unusual activity on the filtering logs

7.23.4 there is failure in the software or abuse of the system

7.23.5 there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks

7.23.6 they notice abbreviations or misspellings that allow access to restricted material

7.24 The DSL will make sure that:

7.24.1 all staff know how to report and record concerns

7.24.2 filtering and monitoring systems work on new devices and services before distributing them

7.24.3 inappropriate content that is blocked is reviewed and updated in line with changes to guidance and safeguarding risks

7.25 E-Safety skills development for staff

7.26 Our staff receive regular information and training on e-Safety issues, including responsibilities for filtering and monitoring.

7.27 All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community. This includes radicalisation and extremism in line with the Prevent Duty.

7.28 New staff receive information on the school's Acceptable Use Agreement as part of their ICT induction.

7.29 All staff incorporate e-Safety activities and awareness within their lessons.

8 E-Safety information for parents/carers

8.1 Parents/carers are asked to read through the Acceptable Use Agreement on behalf of their child.

8.2 Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website and on social media.

8.3 The school website contains useful information and links to sites like Thinkuknow, Childline, CEOP and the CBBC website 'Stay Safe' page.

8.4 The school will send out the relevant e-Safety information through the school website and the school prospectus.

8.5 The school will provide opportunities for parents to discuss e-safety issues annually

9 Teaching and learning

9.1 From 2020 it has been compulsory for all primary aged pupils to receive Relationships Education with online safety explicitly taught within this. Therefore, as part of the curriculum, both PSHE (Relationship Education) and Computing (online safety) we teach pupils the underpinning knowledge and behaviours to enable them to protect themselves and others from online harms and risks which may jeopardise their personal information, lead to unsafe communications or even effect their mental health and wellbeing, regardless of the device, platform or app. We also need to have an understanding of the risks that exist online so we can tailor our teaching and support to the specific needs of our pupils. To this end we ensure that our scheme of work covers those aspects of e-safety highlighted in the document Education for a Connected World Framework which gives age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.

9.2 E-Safety and the Connection to PSHEE & RSE

9.3 Through our E Safety and our PSHEE and RSE curriculum content pupils will be taught what positive, healthy and respectful online relationships look like, the

effects of their online actions on others and knowing how to recognise and display respectful behaviour online. The PSHEE curriculum content also includes citizenship education which covers media literacy - distinguishing fact from opinion as well as exploring freedom of speech and the role and responsibility of the media in informing and shaping public opinion. It also supports teaching about the concept of democracy, freedom, rights, and responsibilities.

9.4 This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

9.5 Curriculum Content

9.6 The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats. It is therefore important for us to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. Our curriculum will cover the following underpinning knowledge and behaviours:

9.6.1 How to evaluate what they see online;

9.6.2 How to recognise techniques used for persuasion or manipulation;

9.6.3 Online behaviour – This will enable pupils to understand what acceptable and unacceptable online behaviour look like and emphasise that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. It also looks at why people behave differently online;

9.6.4 How to identify online risks – This will enable pupils to identify possible online risks and make informed decisions about how to act;

9.6.5 How and when to seek support – This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

9.7 Teaching must always be age and developmentally appropriate. For advice on what is age appropriate the DfE document Education for a Connected World Framework includes age specific advice about the online knowledge and skills

that pupils should have the opportunity to develop at different stages of their lives, including:

9.7.1 How to navigate the internet and manage information;

9.7.2 Copyright and ownership;

9.7.3 Privacy and Security and covers;

9.7.4 How to stay safe online including;

9.7.5 Wellbeing.

9.8 Whilst the above will provide pupils with a solid foundation to navigate the online world in an effective and safe way we will tailor our teaching and support to the specific needs and online risks faced by our pupils. To do this teachers should, with specific pupils in mind, cross reference our current provision with local trends.

9.9 Considering individual pupils and classroom climate

9.10 As with any safeguarding lessons or activities, we will always consider the potential that a child (or more than one child) in the class may be suffering from online abuse or harm in this way. Where we are already aware of a child who is being abused or harmed online, teachers will carefully plan any lesson to consider this, including not drawing attention to that child in a way that would highlight or publicise the abuse. It is good practice to include the Designated Safeguarding Lead (or a deputy) when considering and planning any safeguarding related lessons or activities (including online) as they will be best placed to reflect and advise on any known safeguarding cases, and how to support any pupils who may be especially impacted by a lesson.

9.11 It is important to create a safe environment in which pupils feel comfortable to say what they feel. If a pupil thinks they will get into trouble and/or be judged for talking about something which happened to them online they may be put off reporting it and getting help.

9.12 In some cases, a pupil will want to make a disclosure following a lesson or activity. The lesson may have provided the knowledge that enabled the pupils to realise they are being abused or harmed and/or give them the confidence to say something. This is why it is essential that all pupils are clear what our reporting mechanisms are.

9.13 Vulnerable pupils

9.14 Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. If these issues are applicable to any cohort we will tailor our offer to ensure these pupils receive the information and support they need. The following resources are helpful in this regard:

9.14.1 Vulnerable Children in a Digital World - Internet Matters Children's online activities, risks and safety - A literature review by the UKCCIS Evidence Group section 11 STAR SEN Toolkit - Childnet

10 Managing IT access, systems and use

10.1 Information system security

10.2 The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

10.3 The capacity of the School's ICT systems and their security will be reviewed regularly.

10.4 Virus protection will be updated regularly.

10.5 Security strategies will be discussed regularly.

10.6 Email use within school

10.7 Pupils may only use approved e-mail accounts on the school system.

10.8 Pupils must immediately tell a teacher if they receive offensive e-mails.

10.9 Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission and if permission is given then the pupils would be accompanied by an adult.

10.10 Staff E-mails sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper.

10.11 The forwarding of chain letters is not permitted.

10.12 Pupils may not e-mail staff unless specifically asked to do so for a curriculum activity.

10.13 Published content and the school website

10.14 The contact details on the website should be the school address, e-mail and telephone number. Staff or pupil's personal information will not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

10.15 Publishing pupil's images and work

10.16 Photographs of pupils may only be taken on school devices. Staff must not use their personal devices for this purpose.

10.17 Written permission from parents or carers will be obtained before named photographs of pupils are published on the school website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where the consent could be an issue.

10.18 Parents/carers may withdraw permission in writing at any time.

10.19 Photographs that include pupils will be selected carefully.

10.20 Pupils full names will not be issued anywhere on the school website, particularly in association with photographs.

10.21 Pupils' work can only be published by outside agencies with the permission of the pupil and parents.

10.22 Photographs taken by parents/carers for personal use

10.23 In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner.

10.24 Social networking and personal publishing

10.25 Teachers must be vigilant in looking for the risk of a pupil being radicalised through social media. The document Radicalisation, extremism and terrorism gives helpful advice.

10.26 The school will block/filter access to social networking sites. (Network Manager/Marketing excluded)

10.27 Newsgroups will be blocked unless a specific use is approved.

10.28 Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to any unknown individuals.

10.29 Our pupils are asked to report any incidents of bullying to the school.

10.30 School staff should not add children as "friends" if they use these sites. If a pupil approaches them online the member of staff should let the DSL know.

10.31 School staff are encouraged to be 'professional' and to consider adding parents as friends on social media is inappropriate and to be discouraged. Staff are given guidelines to keep their social media pages 'private'.

10.32 This also includes 'liking' pages on the school's social media accounts.

10.33 Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils and only moderated social networking sites should be used for this age range. Parents will be informed about that the minimum age for accessing most well-known sites is 13 (Y8).

10.34 Parents will be made aware of any child that is under the restricted age, using social media networks.(i.e. Twitter, Facebook)

10.35 Managing filtering and monitoring

10.36 The school ensures systems to protect pupils are reviewed and improved.

10.37 Monitoring user activity is an important part of providing a safe environment. Unlike filtering, it does not stop users from accessing material through internet searches or software.

10.38 All staff must proactively monitor pupils' use of the internet - as they would actively monitor pupils' play at breaktime. Staff must also be proactive in risk assessing the topics the class are covering and consider if innocent searches prompted by genuine curiosity might lead to accidentally harmful search results. Staff must ensure that either pupils are arranged so that their screens can be seen or that the teacher moves and circulates so the teacher can visually monitor what pupils are doing.

10.39 If pupils discover an unsuitable site, it must be reported to the class teacher, ICT teacher and DSL. If staff discover an unsuitable site, it must be reported to the

DSL and then reported to the IT Manager via the following form found here. It should then be reported to the parents.

10.40 When an incident occurs staff must firstly deal with the incident ascertaining the harm, to whom, and prevent further harm or spread. Next the member of staff should save the http address, record the process that occurred; e.g. ask the pupil what they searched for. The first responder should try and establish the extent of the breach as should the DSL and the IT manager after the initial incident - looking for if this breach had happened before without detection or if it was wider than first thought. Members of staff can ask: is this all they have seen? What else have they done? Who else is involved both in and out of school. Ensure that the child isn't shamed and avoid saying anything like 'you know you shouldn't …' as telling them off will prevent them reporting incidents.

10.41 The IT manager will log the breach and report this to the Compliance Committee, chaired by the Safeguarding Governor, at the next meeting along with actions taken to remedy the situation and to prevent similar situations. The IT manager will assist the DSL in investigating how the incident occurred in order to learn lessons. This will be reported to the compliance committee.

10.42 Lessons learnt will be disseminated to the wider community via staff meetings and if necessary parent information events.

10.43 If necessary, the pastoral lead will be informed and take the lead helping the child deal or cope with what they have experienced.

10.44 IT staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

10.45 The DSL will run regular reports to ascertain any risk to staff or pupils of radicalisation, extremism and terrorism. The IT Manager will manually view the IT activity once a day and record any observations on this form.

10.46 Appropriate filtering is in place to ensure that pupils are unable to access terrorist and extremist material online through school servers.

10.47 If staff wish to make a change to the monitoring or filtering systems this must be requested by using the following form.

10.48 Annually the board will consider the school's Monitoring Plan ie the use of both technical and manual monitoring solutions considering the following:

10.48.1 student age

10.48.2 student risk profile

10.48.3 whether screens are easy to see

10.48.4 number of devices in use

10.48.5 whether devices are used off-site, for example, at home

10.49 For monitoring to be effective it must pick up incidents that are of concern urgently, usually through alerts or observations, allowing prompt action to be taken and the outcome recorded.

10.50 The designated safeguarding lead (DSL) is responsible for any safeguarding and child protection matters that are identified through monitoring.

10.51 The monitoring plan will include how we monitor pupils when using school-managed devices connected to the internet. This could include:

10.51.1 device monitoring using device management software

10.51.2 in-person monitoring in the classroom

10.51.3 network monitoring using log files of internet traffic and web access

10.52 As a minimum, the DSL will check the monitoring reports weekly.The IT Manager will notify the DSL immediately when an incident is classed as high-risk, for example, those of a malicious, technical or safeguarding nature.

10.53 The DSL will make sure that everyone using the school's network knows that filtering and monitoring processes are in place.

10.54 Your monitoring plan should include how you communicate with staff about accepted ways of responding to incidents, including:

10.55 how to deal with incidents

10.56 who should lead on any actions

10.57 when incidents should be acted on, in line with your school's policy – read the first standard about filtering and monitoring roles and responsibilities to help with this

10.58 Incidents will be recorded on the daily monitoring log and includes what action was taken and the outcomes. This to help leaders understand the effectiveness of your filtering and monitoring plan.

10.59 Staff must:

10.59.1 provide effective supervision

10.59.2 take steps to maintain awareness of how devices are being used by pupils

10.59.3 report any safeguarding concerns to the DSL

10.60 Managing emerging technologies

10.61 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before its use in school is allowed.

10.62 Pupils are not allowed to bring personal mobile devices/phones/smart watches to school. Any phones/watches/devices that are brought to school will be sent to the school office and kept there until the end of the day.

10.63 The sending of abusive or inappropriate text messages outside school is forbidden.

10.64 Staff will not contact pupils directly by phone. All communication by phone must be with pupils' parents or careers. When telephoning parents or careers, staff will use a school phone.

10.65 Protecting personal data

10.66 The school will collect personal information about you fairly and will let you know how the school and local authority will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians if it is necessary, to pass information beyond the school or education authority. For other members of the community the school will tell you in advance if it is necessary to pass the information onto anyone else other than the school or local authority.

10.67 The school will hold personal information on its systems for as long as you remain a member of the school community and hold it until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with GDPR.

10.68 You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

10.69 Authorising Internet access

10.70 Pupil instruction is responsible and safe use should precede any Internet access and all pupils must have notice of the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules.

10.71 Access to the Internet will be directly supervised access to specific, approved on-line materials.

10.72 All parents will be asked to sign Acceptable Use Agreements for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.

10.73 All staff must read and agree in writing to adhere to the Acceptable Use Agreement for staff before using any ICT resource. This Acceptable Use Agreement form will be discussed at the beginning of each term.

10.74 Password security

10.75 Adult users are provided with an individual network and email login username and password, which they are encouraged to change periodically.

10.76 All pupils are provided with a GAFE user name and a password.

10.77 Pupils from Nursery are given access to GAFE. Children in Year 1 are given access to their email account for the sending of internal email only. Pupils from Year 4 - 6 are allowed to email externally outside of our domain.

10.78 Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

10.79 Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

10.80 Assessing risks

10.81 The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can not accept liability for the material accessed or any consequences of Internet access. The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

11 Appendix A: Acceptable use agreements

11.1 The acceptable use policies for pupils and staff can be found by clicking on the links below:

11.1.1 EYFS / KS1

11.1.2 KS2

11.1.3 STAFF

12 Appendix B: How is technology used to bully?

12.1 Technology can be used both positively and negatively. The table below explores the range of ways today's technology can be used.

Technology:	Great for:	Examples of misuse:
Mobile phones 	Keeping in touch by voice or text, taking and sending pictures and film, listening to music, playing games, going online and sending emails. Useful in emergency situations and for allowing children a greater sense of independence.	Sending nasty calls or text messages, including threats, intimidation, harassment. Taking and sharing humiliating images. Videoing other people being harassed and sending these to other phones or Internet sites.
Instant Messenger (IM) 	Text or voice chatting live with friends online. A quick and effective way of keeping in touch even while working on other things.	Sending nasty messages or content. Using someone else's account to forward rude or mean messages via their contacts list.
Chat rooms and message boards 	Groups of people around the world can text or voice chat live about common interests. For young people, this can be an easy way to meet new people and explore issues which they are too shy to talk about in person.	Sending nasty or threatening anonymous messages. Groups of people deciding to pick on or ignore individuals. Making friends under false pretences – people pretending to be someone they're not in order to get personal information that they can misuse in a range of ways – e.g. by spreading secrets or blackmailing.
Email 	Sending electronic letters, pictures and other files quickly and cheaply anywhere in the world.	Sending nasty or threatening messages. Forwarding unsuitable content including images and video clips, or sending computer viruses. Accessing someone Else's account, e.g. to forward personal emails or delete emails.
Web cams 	Taking pictures or recording messages. Being able to see and talk to someone live on your computer screen. Bringing far-off places to life or video conferencing.	Making and sending inappropriate content. Persuading or threatening young people to act in inappropriate ways. Using inappropriate recordings to manipulate young people.
Social network sites 	Socialising with your friends and making new ones within online communities. Allowing young people to be creative online, even publishing online music. Personalising homepages and profiles, creating and uploading content.	Posting nasty comments, humiliating images / video. Accessing another person's account details and sending unpleasant messages, deleting information or making private information public. Groups of people picking on individuals by excluding them. Creating fake profiles to pretend to be someone else, e.g. to bully, harass or get the person into trouble.
Video hosting sites 	Accessing useful educational, entertaining and original creative video content and uploading your own.	Posting embarrassing, humiliating film of someone.
Virtual Learning Environments (VLEs)	School site, usually available from home and school, set up for tracking and recording student assignments, tests and activities, with message boards, chat and IM.	Posting inappropriate messages or images. Hacking into someone else's account to post inappropriate comments or delete schoolwork.
Gaming sites, consoles and virtual worlds 	Live text or voice chat during online gaming between players across the world, or on handheld consoles with people in the same local area.Virtual worlds let users design their own avatars – a figure that represent them in the virtual world.	Name-calling, making abusive / derogatory remarks. Players may pick on weaker or less experienced users, repeatedly killing their characters. Forwarding unwanted messages to other devices in the immediate vicinity.

13 Appendix C - Education at Home

13.1 Where children are being asked to learn online at home SPS will have reference to the advice contained within:

13.1.1 safeguarding-in-schools-collegesand-other-providers; and

13.1.2 safeguarding-and-remote-education.