E-Safety Policy	
Review Frequency	Annual
Reviewed and approved by	Full Governing Body
Date	April 2024
Headteacher Signature	Lauren Hill
Chair of Governors Signature	Ruth Downes Sarah Thompson
Date of next review	September 2024

E-Safety Policy 2024

Introduction

E-Safety encompasses the use of new technologies, internet and electronic communications such as learning platforms, mobile phones, video conferencing, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's E-Safety Policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security, Acceptable Use and Communication Policy. E-Safety also relates to the school Child Protection and Safeguarding Policy.

Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and Responsibilities

1. Governors

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The governor who oversees online safety and safeguarding is **Mrs Rosy Astbury.**

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on Acceptable Use of the School's ICT systems and the internet (appendix 3)
- Review termly online safety reviews (collated from the monitoring logs) provided by the Headteacher.

2. Headteacher and Seniors Leaders

The Headteacher is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the school. The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community. The Headteacher is responsible for buying the necessary filtering and monitoring software.

- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles (see appendix 6).

3. Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) are set out in our Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, school's technician and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's behaviour policy.
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher and/or governing body
- Reviewing events that are flagged by our monitoring system E set Internet Security

This list is not intended to be exhaustive.

4. ICT/Computing Lead

Together with the Headteacher and Senior Leaders, the Computing and E-safety Lead and the school's technician are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- Appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- That the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- That a full security check and monitoring the school's ICT systems on a regular basis.
- Potentially dangerous sites are blocked and, where possible, preventing the downloading of potentially dangerous files (see appendix 6).
- That any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- That any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- That the school meets required online safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That the web filtering statement, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, internet, remote access, email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader and E-Safety Leader.
- Discuss any trends which have been identified by the monitoring and filtering system. Review these through the online safety curriculum, of relevant (appendix 6).
- Updating the risk assessment for internet use

This list is not intended to be exhaustive.

5. Teaching and Support Staff

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on Acceptable Use of the school's ICT systems and the internet (appendix 3) and ensuring that pupils follow the school's terms on acceptable use (appendix 1).
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

This list is not intended to be exhaustive.

6. Parents and Carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1).
- Read and agree to the terms of the acceptable use of the internet for parents and carers (appendix 2).

Parents can seek further guidance on keeping children safe online from the following organisations and websites…

UK Safer Internet Centre: What are the issues?
https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Childnet International: Hot Topics
http://www.childnet.com/parents-and-carers/hot-topics

Childnet International: Parent Factsheet
http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Parents should also familiarise themselves with the E-Safety section of the school website where information is frequently updated.
https://www.stmatthewsceprimary.com/e-safety/

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours.

Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Annual E-Safety Training for parents and carers will be arranged via links on the school website and workshops hosted by our PCSO and E-Safety Lead.

Additionally, we will provide information and awareness to parents and carers through:

- Curriculum activities
- Letters and newsletters
- Information on the school website and the school's Facebook account
- Parents/carers evenings/sessions
- High profile events/campaigns for example: Safer Internet Day, Anti-Bullying Week etc…
- Reference to the relevant web sites/publications

7. Visitors and Community Users

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

E-Safety depends on effective practice at a number of levels:

- Responsible ICT (Information & Communication Technologies) use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of E-Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from an approved Internet Service Provider using suitable filtering.

- National Education Network standards and specifications.

Our E-Safety Policy and its implementation is updated on an annual basis. Our E-Safety Policy has been written in conjunction with staff at school, building on the Cheshire E-Safety Policy and government guidance. It has been agreed by senior management and approved by governors. It will be shared with parents/carers.

Our E-Safety Coordinator is:

- Miss Lauren Hill (Headteacher)

The coordinator works closely with the Local Authority (LA) ICT support service technicians.

Key LA Contacts:

- Child Protection Services
- Primary ICT Adviser

Preventing Extremism and Radicalisation

Our Preventing Extremism and Radicalisation policy is intended to provide a framework for dealing with issues relating to vulnerability, radicalisation and exposure to extreme views. We recognise that the internet and in particular social media are used to radicalise and recruit young people. This policy should be read in conjunction with our Preventing Extremism and Radicalisation policy and the Home Office publication 'How Social Media is used to encourage travel to Syria and Iraq- briefing note for schools.' (July 2015).

In the same way teachers are vigilant about signs of possible physical or emotional abuse in any of our pupils, any concerns for the safety of a specific young person at risk of radicalisation are dealt with using the schools safeguarding procedures. We have a Prevent Lead who can also provide support.

Teaching and Learning

Why Internet use is important…

- The Internet is an essential element in 21st century life for education, business and social interaction. The School has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil and family use and will include filtering appropriate to the age of pupils.
- Pupils and families will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

i. Information system security

- School ICT systems and security will be reviewed regularly. (Please refer to Appendix 2).
- Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily.
- We have adopted Cheshire West and Cheshire's security standards.

ii. E-mail

- Pupils may only use approved e-mail accounts on the school system. The school does not permit individual pupils to have their own email accounts. Accounts are set up on a class basis.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

iii. Published content and the school website

- The contact details on the website should be the school's address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility for each website in conjunction with the ICT coordinator and link ICT Governor and ensure that content is accurate and appropriate.

iv. Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

v. Social Networking and Personal Publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents may be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

vi. Managing Filtering

- The school will work with the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety (ICT) Coordinator. The Local Authority, as the Internet Service Provider, includes filtering at a county level. If sites are blocked there is a mechanism to release sites on approval by the Advisory team. Where schools find sites or content that is inappropriate, they should contact the ICT Service Desk on 0300 123 5121 and ask for the site to be blocked.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. (Please see Appendix 2).

vii. Managing Videoconferencing

- School uses Zoom for remote lessons and parents' evenings when required.
- Invitations are sent via the children's secure homework page where they have to login to School Spider to access their account. For parent's evening it is sent via secure email.
- Teachers use the waiting room function and ask that people use their real name so they are easily identifiable. Anyone we don't recognise is not admitted and cannot join the call.
- Parents are asked to supervise children at all times when engaging with a live Zoom.

viii. Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Pupils are not allowed to bring mobile phones into school.
- Staff will not use personal equipment or non-school personal electronic accounts when contacting students. The school phone will be used where contact with pupils is required.

ix. Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018. See reference to General Data Protection Regulation (GDPR) Policy

Policy Decisions

i. Authorising Internet Access

- All staff must read and sign the **'Staff Information Systems Code of Conduct'** before using any school ICT resource.
- All pupils and their parents/carers must read and agree to the **'Pupils' Safety Rules'**. This will be issued to parents/carers with the school's Home School Agreement and Parents will be asked to agree to and return a consent form with respect to the 'Pupils Safety Rules'. For children in Year 3 and above, the children will be asked to sign this themselves.
- The school will keep a central record of all staff and pupils who are granted Internet access. The record will be kept up to date. For instance a member of staff may leave or a pupil's access be withdrawn. It is the Headteacher's responsibility to ensure that the record is kept up to date so that it can be easily referred to.
- Within the primary school access to the Internet will be supervised. Lower down the school access will be to specific approved online materials.

ii. Assessing Risks

- 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. Neither the School nor the local authority can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT provision to establish if the E-Safety Policy is adequate and that its implementation is effective.

iii. Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff/Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and referred to the Headteacher as Designated Safeguarding Person or the School. Pupils and parents will be informed of the complaints procedure and the School Complaints Policy will be followed.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

iv. Communications Policy

Introducing the E-Safety Policy to pupils

- E-Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety Policy

- All staff will be given the school E-Safety Policy and its importance explained. A copy will also be held in the central policy files – curriculum policy files
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting Parents' Support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school website.

Cyberbullying

Cyberbullying 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also our Behaviour Policy.)

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

Preventing and Addressing Cyberbullying
The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, families are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should families comment on any activities involving other *students/pupils* in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on a website or Facebook, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/Facebook.

To help prevent cyberbullying, 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 cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyberbullying and the issue will be addressed in assemblies.

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

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/ leaflets on cyberbullying to parents so that 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 cyberbullying, 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 consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining Electronic Devices
School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

Acceptable Use Agreements

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1, 2 and 3). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the School's Acceptable Use Policy and acceptable use agreements in appendices 1, 2 and 3.

Staff using work devices outside of school
Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the ICT technician. Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Pupils

Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email					X		X	
Unauthorised downloading or uploading of files	X			X				
Allowing others to access school network by sharing username and passwords	X						X	
Attempting to access or accessing the school network, using another student's / pupil's account	X						X	
Attempting to access or accessing the school network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the school into		X		X				X

disrepute or breach the integrity of the ethos of the school								
Using proxy sites or other means to subvert the school's / academy's filtering system					X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

Staff

Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					X

Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material				X			X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X					X	X

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 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".
- 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 are carried out
- 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 safe keeping 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.

Social Media – Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party.

Reasonable steps to prevent predictable harm must be in place.

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, families or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

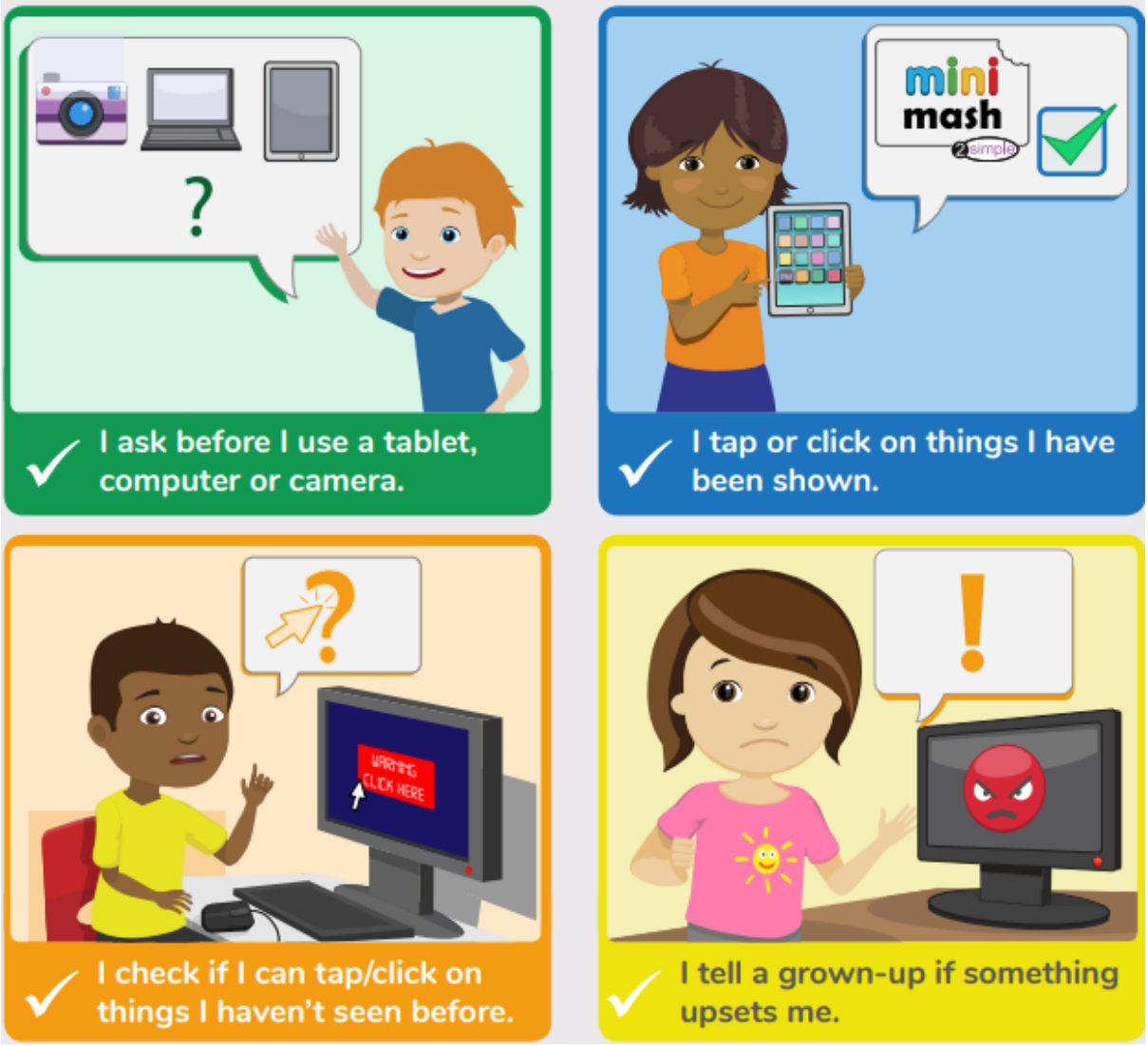
The school's use of social media for professional purposes will be checked regularly by the Headteacher to ensure compliance with the Social Media, Data Protection, Communications, practices.

Appendix 1: Acceptable Use Agreement - Pupils

Acceptable Use of the School's ICT Systems and Internet: Agreement for Pupils in EYFS

Name of pupil:

When I use the school's ICT facilities (computers, tablets and equipment) and accessing the internet in school, I will always do the following:



Signed (child):	**Date:**

Acceptable Use of the School's ICT Systems and Internet: Agreement for Pupils in KS1

Name of pupil:

At school:

- I will only visit websites that I have been directed to.
- I will always ask permission before going on a device.
- I will protect my personal information.
- I understand that the school will monitor the websites I visit.
- I will always communicate in a polite and respectful way.
- I will tell someone immediately if I see something that upsets me.

At home:

- I will not use mean or rude language when communicating online.
- I will not share my password with others or log in using someone else's name and password.
- I will not bully other people.

Signed (child):	**Date:**

Acceptable Use of the School's ICT Systems and Internet: Agreement for Pupils in KS2

Name of pupil:

When I use the school's ICT facilities (computers, tablets and equipment) and accessing the internet in school, I will not:

- Use them for a non-educational purpose.
- Use them without a teacher being present, or without a teacher's permission.
- Access any inappropriate websites.
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity).
- Use chat rooms.
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer.
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

Additionally:

- I understand that the school will monitor the websites I visit.
- I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
- I will always use the school's ICT systems and internet responsibly.

When I communicate online, at home and at school, I will not:

- Use mean or rude language when communicating online.
- Share my password with others or log in using someone else's name and password
- Bully other people.

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: Acceptable Use Agreement Parents and Carers

Acceptable Use of the School's ICT Systems and Internet: Agreement for Parents and Carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. **The school uses the following channels:** • Our official Facebook accounts • School Spider notifications for parents/carers (for school announcements and information) • Emails from school Parents/carers may also set up independent channels to help them stay on top of what's happening in their child's class. For example, group chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure **I will not:** • Use private groups, the school's Facebook page or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the school's Facebook page or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable Use Agreement Staff, Governors, Volunteers and Visitors

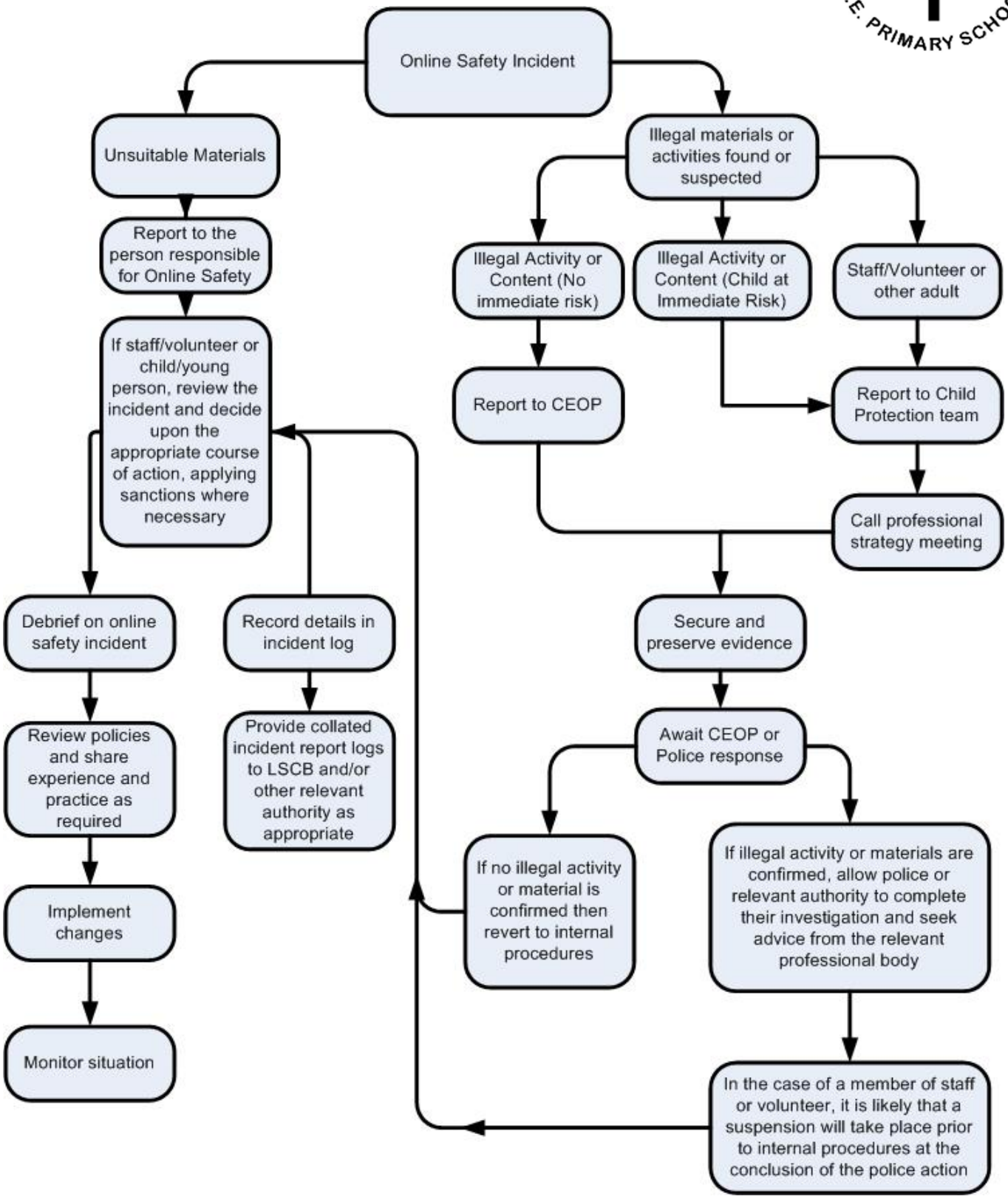
Acceptable Use of the School's ICT Systems and Internet: Agreement for Staff, Governors, Volunteers and Visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details	
✓I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. ✓ I agree that the school will monitor the websites I visit. ✓ 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 let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and 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.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Online Safety Training Needs – Self Audit for Staff

Online Safety Training Needs Audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 6: Filtering and Monitoring Checklist

Filtering and monitoring provided by: Talk Straight / Eset Internet Security



Appendix 7: Annual Checklist

CHECKS TEMPLATE	DATE OF CHECK	WHO DID THE CHECK	RESULTING ACTIONS
Have we checked that our filtering and monitoring system is still fit for purpose? Test Your Internet Filter | SWGfL Test Filtering			
Is the system running and working?			
Have we checked that our filtering and monitoring system works on: › All devices › New devices and services before they're given to staff or pupils			
Have we reviewed the list of blocked sites on our network? Is this list still accurate/does it reflect any changes to safeguarding risks?			
Does our filtering system adhere to the requirements? (Get your checklist of the requirements here)			
Does our monitoring system adhere to the requirements? (Get your checklist of the requirements here)			

Appendix 8: Internet Use - Possible Teaching and Learning Activities

Activities	Key E-Safety Issues
Creating web directories to provide easy access to suitable websites.	• Parental consent should be sought. • Pupils should be supervised. • Pupils should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	• Parental consent should be sought. • Pupils should be supervised. • Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail.	• Pupils should only use approved e-mail accounts. • Pupils should never give out personal information. • Consider using systems that provide online moderation e.g. The Learning Platform.
Publishing pupils' work on school and other websites.	• Pupil and parental consent should be sought prior to publication. • Pupils' names and other personal information should be omitted.
Publishing images including photographs of pupils.	• Parental consent for publication of photographs should be sought. • Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.
Communicating ideas within chat rooms or online forums.	• Only chat rooms contained with the schools Learning Platform and linked to educational use and that are moderated should be used. • Access to other social networking sites should be blocked. • Pupils should never give out personal information.