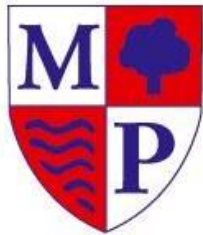


Mersey Park Primary School



Digital Safety Policy



Approved by:	Governing Body	Date: September 2027
Last reviewed on:	September 2026	
Next review due by:	September 2027	

Contents

1. Aims	2
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	6
5. Educating parents/carers about online safety	6
6. Cyber-bullying	7
7. Acceptable use of the internet in school	9
8. Pupils using mobile devices in school	9
9. Staff using work devices outside school	9
10. How the school will respond to issues of misuse	10
11. Training	10
12. Monitoring arrangements	11
13. Links with other policies	11
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	12
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)	14
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)	16
Appendix 4: online safety training needs – self-audit for staff	18
Appendix 5: online safety incident report log	19
Appendix 6: Flowchart for responding to Digital Safety incidents and Risk Assessment	20

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE'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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Mr R Cook.

All governors will:

- Ensure 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)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher, Mrs Thomas, is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL – Ms L White) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) 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 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 board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Computing leads

The Computing leads, Mrs V Inman and Mrs J Robertson, along with the ICT Technician and Computing Team are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) 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

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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 (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by logging any incidents and then following up that action has been taken
- Following the correct procedures by directly speaking to the DSL or Headteacher if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/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 (appendices 1 and 2)

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

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)

3.7 Visitors and members of the community

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).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant and revisited on a regular basis.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

All classes will display an age-appropriate SMART rules poster in class. The class e-Safety Cadet will provide a reminder in each lesson about the safe and responsible use of the internet, in any relevant lessons.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website and X feed (formerly Twitter). This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings, productions and other workshops.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes during PSHE and Computing lessons. The children will also access work on cyber-bullying through the year during themed weeks.

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

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

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

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

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

6.3 Examining electronic devices

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

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or

- Is evidence in relation to an offence

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

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

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

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

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

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

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

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy

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

6.4 Artificial intelligence (AI)

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

Mersey Park Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Mersey Park Primary School will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school. AI will not be used with pupils unless explicit permission has been sought. See AI policy for more detail.

7. Acceptable use of the internet in school

All pupils, parents/carers, 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 to 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Playtimes/Lunchtime
- Clubs before or after school, or any other activities organised by the school

Any mobile devices in school must be handed to the floor leader/class teacher for safe keeping until the end of the school day, which is in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Computing leads or the ICT Technician.

10. 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 our policies on behaviour, ICT and internet acceptable use. 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 / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Computing leads. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- AI policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Mersey Park Primary School

Acceptable User Policy -

Pupils and Parents/Carers



Mersey Park Primary School promotes the use of technology as all pupils will need these skills and knowledge in whatever field of work they enter when they become an adult. We ensure that our school IT network is robust and resilient and we do our utmost to ensure the safety of children when using it. It is important that pupils abide by the school rules when using technology in school and inform a member of staff immediately, if they become aware of any misuse.

This is the Acceptable User Policy (AUP) for our school. It highlights appropriate and inappropriate behaviour when using all technology in school and shows how we want pupils to behave when using IT. Any misuse will result in pupils being temporarily banned from using the school network.

Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form your child will not be able to have full access to the IT systems in school.

For Pupils:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I select a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed - Pupil: _____

Pupil name: _____

Class: _____

For Parents/Carers:

- I agree to support and uphold the principles of this policy in relation to my child and their use of technology and the Internet, at home and at school.
- I agree to uphold the principles of this policy in relation to my own use of the Internet, when that use is related to the school, employees of the school and other students at the school.
- I will not use social media to make complaints or derogatory comments about the school. If I have a complaint I will follow the correct complaints procedure (see Concerns & Complaints Policy).
- Images of pupils will only be taken, stored and used for personal memories or school purposes in line with school policy. Images will only be used on the Internet, in the press, or in media, with specific written permission from the parent/carer of every pupil on the photograph.

Signed - Parent/Carer: _____

Parent/Carer name: _____

Date: _____

Mersey Park Primary School

Acceptable User Policy -

Pupils and Parents/Carers



Mersey Park Primary School promotes the use of technology as all pupils will need these skills and knowledge in whatever field of work they enter when they become an adult. We ensure that our school IT network is robust and resilient and we do our utmost to ensure the safety of children when using it. It is important that pupils abide by the school rules when using technology in school and inform a member of staff immediately, if they become aware of any misuse.

This is the Acceptable User Policy (AUP) for our school. It highlights appropriate and inappropriate behaviour when using all technology in school and shows how we want pupils to behave when using IT. Any misuse will result in pupils being temporarily banned from using the school network.

Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form your child will not be able to have full access to the IT systems in school.

For Pupils:

Using Technology in School

- I will only use the school Internet and network for my school work or when a teacher has given permission.
- I will not try and bypass the schools Internet settings.
- I will only use a given email address when using email in school. I will always log off my email account when finished
- I will not look at, change or delete other people's work or files.
- I will be careful with all IT equipment such as keyboards, mice, headphones and when turning a computer on or off.
- I will be sensible when using mobile technologies and follow the rules about moving about the school when using them.
- I will follow the rules about bringing my own personal device into school e.g. smartphone, smartwatch.

Security, Passwords & Copyright

- I will not share my username or passwords. My password will use both letters and numbers.
- I will be careful when opening emails from people I don't know and I will ask an adult if I'm unsure whether to open it.
- I won't upload or download any pictures, writing or movies which might upset people or make other people think the school is a bad place.
- I will use non-copyrighted images and music from the Internet when creating documents, presentations or other media.
- I won't try to install software onto the school network because it might have a virus on and cause a lot of damage. Instead I will ask a teacher for advice.

Online Behaviour & Safety

- I won't give out my personal details, such as my name, age, address, school name or phone number on the Internet or when registering for a software app.
- I won't meet people I've met on the Internet unless I have told my parents and they come with me.
- I will make sure all my contact with other people at school is responsible. I will not cyber bully pupils, teachers or other members of staff.
- I won't look for or look at unpleasant or inappropriate web sites or software apps. I will check with a teacher if I think it might be unsuitable.
- I know that everything I do on the computers at school is recorded and that the school can talk to my parents if a teacher is worried about my online safety.
- I will try to follow these rules all the time because I know they are designed to keep me safe.

Signed - Pupil:

Pupil name:

Class:

For Parents/Carers:

- I agree to support and uphold the principles of this policy in relation to my child and their use of technology and the Internet, at home and at school.
- I agree to uphold the principles of this policy in relation to my own use of the Internet, when that use is related to the school, employees of the school and other students at the school.
- I will not use social media to make complaints or derogatory comments about the school. If I have a complaint I will follow the correct complaints procedure (see Concerns & Complaints Policy).
- Images of pupils will only be taken, stored and used for personal memories or school purposes in line with school policy. Images will only be used on the Internet, in the press, or in media, with specific written permission from the parent/carer of every pupil on the photograph.

Signed - Parent/Carer:

Parent/Carer name:

Date:

Mersey Park Primary School

Acceptable User Policy:



For all staff, governors and external contractors accessing the school network on site or remotely.

Mersey Park Primary School promotes the positive use of technology in school and assists in developing pupils' knowledge and understanding of digital devices and the Internet. We ensure that our school IT network is robust and resilient and staff have a duty of care to safeguard pupils when using technology in school. Any misuse of technology by a pupil or member of staff must be reported to the Designated Safeguarding Officer, so an investigation can take place.

This is the Acceptable User Policy (AUP) for our school. It highlights appropriate and inappropriate use of all technology in school and shows how we want staff to behave when using IT. The AUP covers the following legislation:

- Malicious Communications Act
- 1988 Data Protection Act 1998
- Computer Misuse Act 1990
- Communications Act 2003
- Sexual Offences Act 2003

Please read carefully and sign at the bottom to show you agree to these terms.

Using Technology in School

- I will only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of a SLT teacher.
- I will monitor the use of all IT in school and report any inappropriate use by pupils or staff to the Designated Safeguarding Officer (DSO).
- I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, extremist, defamatory or copyright infringing.

Security, Passwords & Copyright

- I will not divulge any school related passwords and I will comply with school IT security procedures.
- I will use school email systems for school related communications. I will not use personal accounts for school business.
- I will ensure that personal data is stored securely and in line with the Data Protection Act. I will follow school policy with regard to external logins, encrypted data and not storing school material on personal IT equipment unless stated otherwise.
- I will not install software onto the network or mobile devices unless supervised by the Network Manager or IT support staff.

Social Media

- I must maintain my professionalism at all times when using personal social media and not bring the school or my profession into disrepute by posting unsuitable comments or media when using these sites.
- I must not use social media tools to communicate with current or former pupils, particularly those under the age of 18.
- I will only use authorised school social media accounts to post information to pupils or parents.
- I will ensure there is no means of identifying my employer on my social media profile (place of work or school badges visible).

Mobile Technologies

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode when I have directed time with pupils. I will only make or receive calls in specific places e.g. staffroom, office.
- I will not contact any parents or pupils on my personally-owned device.
- I will NOT use a personally-owned mobile device to take images, video or sound recordings for ANY purpose.
- I will ensure that all school data on devices is password protected and that I have agreed for the IT support staff to erase and wipe data off my device, if it is lost and/or as part of my exit strategy.

Online Professionalism

- I am aware that all network and Internet activity is logged and monitored and that the logs are available to SLT in the event of allegations of misconduct.
- I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, parents or staff on social media or websites in any way which might bring the school into disrepute.
- I will make sure that my Internet presence does not bring the teaching profession into disrepute and that I behave online in line with the Teacher Standards (2012) and other guidelines from the D of E.
- I will champion the school's Digital Safety policy and be a role model for positive and responsible behaviour on the school network and the Internet.
- I will not give my home address, phone number, mobile number, personal social networking details or email address to pupils. All communication with parents should be done by authorised school contact channels.
- Photographs of staff, pupils and any other members of the school community will not be used outside of the internal school IT network unless written permission has been granted by the subject of the photograph or their parent/carer. I will ask the permission of the Head Teacher (on site) or the proprietor of the building (off site) prior to taking any photographs.

Signed:

Name:

Date:

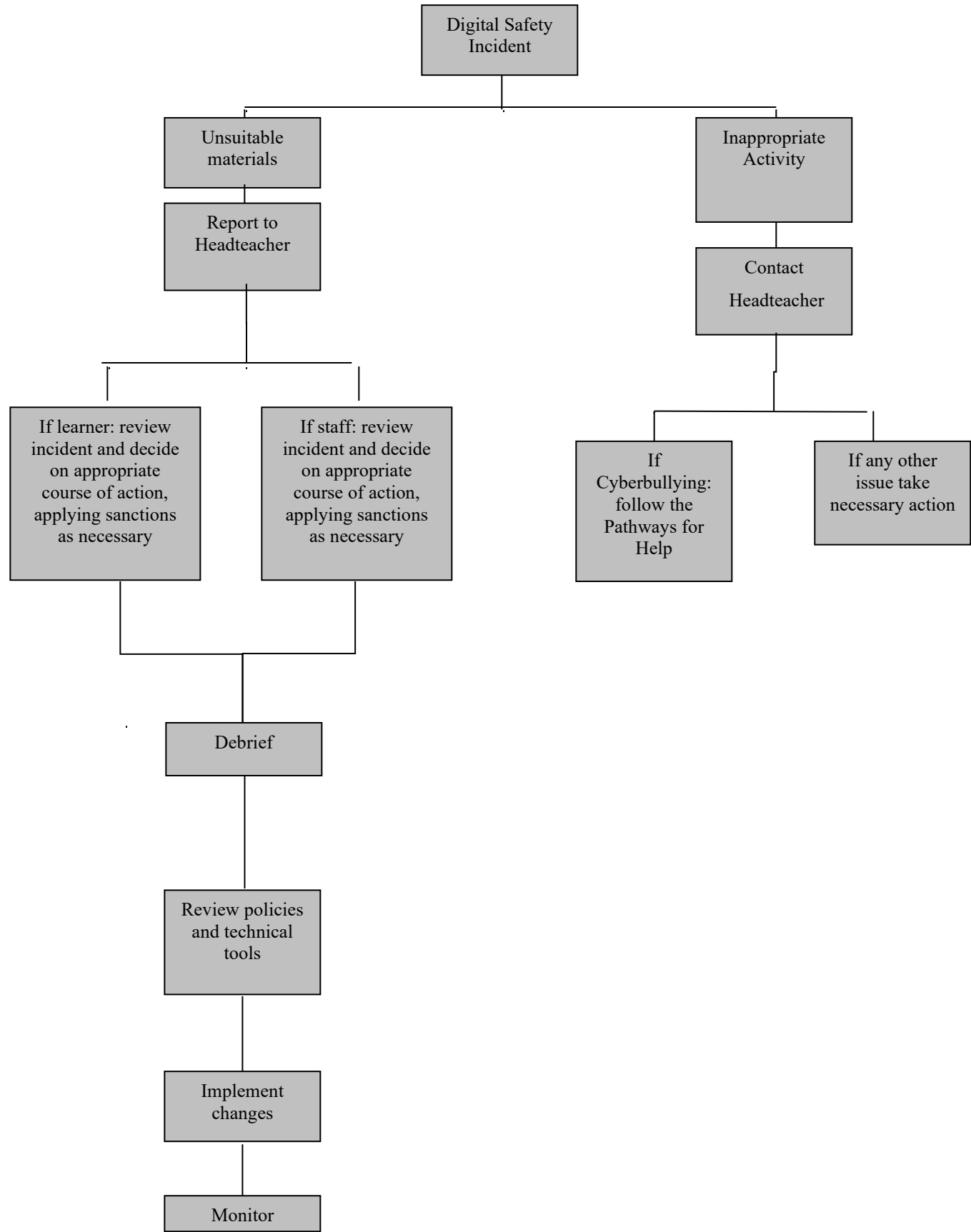
Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 6: Flowchart for responding to Digital Safety incidents and Risk Assessment



Guidance on completing this form is available in the Health & Safety Management Arrangements for Risk Assessment

Location or address		MPPS classrooms		Date assessment undertaken: Autumn 2025	Assessment undertaken by V Inman
Activity or situation		Digital Safety		Review date: Autumn 2026	Signature
1) Hazard (See appendix 2 - H&S Management Arrangements for Risk Assessment)	2) Who can be harmed and how? (See appendix 2 -H&S Management Arrangements for Risk Assessment)	3) Generic Controls – What generic controls exist to reduce the risk? AND (If applicable) Visit Specific Controls		Risk Score Consequence X Likelihood	4) Any further action; This should be included in the action plan on overleaf
Misuse of computers	Pupils – electric shock, damaged equipment potentially causing harm to pupil, access to inappropriate material	Equipment checked for electrical safety Equipment checked for any damage AUP in place for all pupils Digital Safety posters and verbal reminders given Computing curriculum covers Digital Safety and responsible use Supervised/monitored by staff on all activities		2 x 2 = 4	
Cyberbullying	Pupils – messages/images received using modern technology, upsetting	Appropriate behaviour discussed AUP signed e-Safe monitoring explained and in use Ability to limit pupil access if necessary Anti-bullying policy known by children Computing curriculum covers Digital Safety regularly Supervised/monitored by staff on all activities		2 x 2 = 4	Reminders given to pupils about use of Social Media and technology when out of school.
Inappropriate material accessed	Pupils – inappropriate material accessed	Supervised/monitored by staff on all activities Wirral LA filtering Internet only accessed through Safe Search homepage on Safari/Chrome/Internet Explorer All time on devices planned Specific apps/websites to be used – QR codes one way of accessing specific sites Children taught to evaluate content		1 x 2 = 2	

Risk Rating	Action Required
17 - 25	Unacceptable – stop activity and make immediate improvements
10 – 16	Tolerable – but look to improve within specified timescale
5 – 9	Adequate – but look to improve at review
1 – 4	Acceptable – no further action but ensure controls are maintained

Likelihood:

5 – Very likely

4 – Likely

3 – Fairly likely

2 – Unlikely

1 – Very unlikely

- (1) List hazards ***something with the potential to cause harm*** here
- (2) List groups of people who are especially at risk from the significant hazards which you have identified
- (3) List existing controls here or note where the information may be found. Then try to quantify the level of risk ***the likelihood of harm arising*** that remains when the existing controls are in place based on the number of persons affected, how often they are exposed to the hazard and the severity of any consequence. Use this column to list the controls that you might take and develop all or some of that list into a workable action plan. Have regard for the level of risk, the cost of any action and the benefit you expect to gain. Agree the action plan with your team leader and make a note of it overleaf. If it is agreed that no further action is to be taken this too should be noted.

(5) ACTION PLAN