Merridale Primary School

E-Safety and Digital Safeguarding Policy

September 2023-September 2024

School Vision

Technology is an essential part of modern life and that it is a duty to provide pupils with quality technology as part of their learning. Merridale Primary School embraces this challenge and this digital safeguarding policy considers the use of both fixed and mobile devices with internet connections, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, gaming devices and other portable media devices. It will be revised to incorporate new and emerging technologies as they appear.

Aims

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Equality and Diversity

The use of technology is a part of the statutory curriculum and a necessary means of delivering 21st century teaching and learning for staff and pupils. Internet access is an entitlement for all. However, responsible and safe use must be at its core.

Technology in a changing world

Schools are part of a world where technology is integral to the way life is led in the 21st century. Compared to even five years ago the technology available outside school is rapidly increasing. In line with the Gilbert review document 2020 Vision, schools need to increasingly respond to:

- An ethnically and socially diverse society
- Far greater access and reliance on technology as a means of conducting daily interactions and transactions
- A knowledge based economy
- Demanding employers, who are clear about the skills their businesses need and value
- Complex pathways through education and training, requiring young people to make choices and reach decisions.

Why do learners need to be safe working with technology?

As the uses of online technology resources grow, so has the awareness of risks and potential dangers which arise for their use. The school aims to prepare its learners to be able to thrive and survive in this complex digital world. This policy outlines the safeguarding approach to achieve this.

Management of Digital Safeguarding

Clearly stated roles and responsibilities-

- **Governors**

  Governors are responsible for the approval of the Digital Safeguarding and E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Curriculum Committee receiving regular information about online safety incidents and monitoring reports.

- **Headteacher**

The headteacher will ensure that the digital safeguarding/E-safety policy is implemented and will monitor compliance with the policy, and that appropriate roles and responsibilities of the school's digital safeguarding structure is in place. They will ensure regular reports on the monitoring outcomes for digital safeguarding are reported to the governing body.

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the E-safety Co-ordinator.
- The Headteacher and DSL/DDSLs 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 is responsible for ensuring that the E-Safety Safety Coordinator 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 safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

- **Nominated e-safety co-ordinator**

There is an identified e-safety co-ordinator (Computing lead) who is responsible for e-safety developments in school and sharing of practise with staff and the wider community of governors and parents.

This person will be in receipt of current training of the latest guidance and procedures and is the main contact for local authority e-safety networks.

All digital safeguarding incidents within the school need to be reported to this person. They will use the CPOMS behaviour tracker to keep a log of e-safety incidents. Alongside the headteacher, they will make decisions about how to deal with reported incidents and adapt policies where necessary. They will also ensure that appropriate education is put in place as a response.

Network Manager / Technical staff:

The Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority 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.
- the filtering policy (if it has one), 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 / Learning Platform / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and E-Safety Safety Coordinator for investigation.
- that monitoring software / systems are implemented and updated as agreed in school policies

- **E-safety responsibility within subject and management roles**

All staff with subject and management roles have a duty to incorporate e-safety principles in their area of responsibility, deputising to any of the above roles where necessary.

- **Teacher**

All staff understand the need for care and caution when using technology both for academic and social purposes and apply it to teaching and learning situations. They need to work to the agreed guidelines. They have a "front line" monitoring and reporting role for incidents.

- they have an up-to-date awareness of online safety matters and of the current school Digital Safeguarding and E-Safety Policy and practices

- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher, Online Safety Coordinator for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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

- **Learning Mentor**

The learning mentor will work alongside the e-safety co-ordinator to monitor e-safety incidents within school and help to deliver appropriate education to children and parents who are involved.

- **Support Staff**

  As for teaching staff, however, given the nature of their role, learners may find it easier to disclose incidents to them. Support staff should be clear about the reporting procedures and use these when incidents occur.

- **School Council Representatives and Digital Leaders**

  As a responsible member of their class, the school council need to have e-safety as an item on their agenda. These representatives could help to monitor the appropriate use of technology at a learner level within the school.

Procedures

- All staff and members of the school workforce and children will sign an AUP (acceptable use policy) on an annual basis to ensure that all changes have been agreed.
- Children will be taught about the CEOP report abuse button during e-safety lessons. E-safety issues should be reported to class teacher or e-safety co-ordinator.
- A log of e-safety incidents will be kept on the CPOMS behaviour tracker and these will be reviewed termly by the e-safety co-ordinator to ensure that next steps have been implemented.
- If child safeguarding issues arise they will be reported to the safeguarding co-ordinator and procedures as defined in the school's safeguarding policy will be followed.
- If necessary the headteacher and safeguarding co-ordinator will follow appropriate procedures for reporting incidents beyond the school to the LA.
- All staff are entitled to training and support regarding e-safety. This will be delivered on a regular basis and a record of its delivery will be kept.

- E-safety education is built into our RHE and computing curriculum with e-safety education being delivered at an appropriate level on a regular basis. Our e-safety curriculum map outlines objectives taught each year.
- We will endeavour to provide appropriate training for parents and keep a log of training provided.
- If e-safety incidents occur, the e-safety co-ordinator will ensure that appropriate teaching is put in place to respond directly to the incident.
- E-safety teaching will be monitored as part of our teaching and learning policy.
- The incident log will be reviewed to effectively assess the impact of e-safety practise and this will be used to inform future planning.

<u>Risks and Acceptable Behaviours</u>

- General use of the internet

The internet is a vital tool to be used inside and outside of school. However there have to be procedures put into place to ensure appropriate use. At the beginning of each year, children are required to sign an AUP appropriate to their Key Stage, which refers to appropriate internet use.

- Passwords/personal details

Staff and children (in KS2) are given passwords and logon details to access ICT facilities and TEAMS. Staff are encouraged to personalise their password and change it regularly. Children are encouraged to report any occasions when their password may have been compromised so that it can re-set accordingly. In foundation stage and Year 1 children will log on to the school system with a generic username and password which will typically be entered by a member of staff.

- Data Security

We discourage the use of memory sticks especially if they contain sensitive information about children e.g. photographs or personal details. Rather than memory sticks staff are encouraged to use the Learning Platform or the staff shared area for data storage and security. In case of theft, we encourage all staff to not store images of children on their laptops.

- E-mail

Staff use their school email account for any correspondence related to school. Information about pupils should only be sent via email where necessary and staff are encouraged to password protect files containing data about individuals.

- TEAMS

Teams is widely used by staff and children. To ensure digital safety, all users have a personal logon and password that is unique. All users are encouraged not to share their details with anyone particularly when out of school setting. If a password breach occurs the e-safety co-ordinator is responsible for altering the password accordingly. Staff and pupils who leave the school will be removed through the regular running of the SIMs connect tool and this will be monitored by the e-safety co-ordinator.

- Appropriate use of hardware

Staff are given appropriate training when they receive a new piece of hardware. They are asked to sign a laptop agreement when they begin employment at the school.

- Photographs, video and sound recording

At the beginning of their time at Merridale, parents will complete our photography permission form which allows children to be photographed and recorded during their time at school. A central list of permissions is held on the staff shared area and all school staff should be aware its contents. If children are not allowed, then relevant staff will need to be aware and ensure that this is adhered to particularly when children are on out of school visits.

- Copyright

Staff are made aware of copyright issues through appropriate staff training and a digital copyright statement. If they wish to use images or videos then there are 'copyright' free sites such as www.freeplaymusic.com which are accessible. Children will routinely explore copyright issues where appropriate.

- Social networking/cyber bullying

Social networking plays a huge part in today's society. Staff are made aware of the Local Authority view regarding acceptable behaviour - staff should not to make any reference to their job, school or other colleagues on the site and are strongly discouraged from accepting friend requests from current or former pupils under 18 years of age. Any disclosures made regarding cyber bullying that occur either within or outside school should be reported and dealt with the school's anti-bullying policy. Cyber bullying will be covered during e-safety education across year groups. The school has a social media policy in place.

- Mobile phones/technology

Children are discouraged from bringing mobile phones into school unless a parent specifically requests this. If this is the case, then they should be handed in at the main office at the beginning of the day and collect them again at the end of the day. Staff are not permitted to use a mobile phone within the hours 8.30am – 4.30pm except in the PPA room, staff room or school office. Videos and photographs are not to be taken or stored on staff mobile phones unless agreed with the Headteacher. Photos/videos must be removed/downloaded from staff devices after use.

Technical – infrastructure / equipment, filtering and monitoring (see our monitoring and filtering policy for more details)

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

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

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users from Years 3 - 6 will be provided with a username and secure password by the technical support officer *who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password.
- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place.
- The Technical support officer is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- The school has provided differentiated user-level
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. They have a separate logon specifically for temporary guests of the school.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils) and their family members are allowed on school devices that may be used out of school.
- **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured**.

Mobile Technologies (including BYOD/BYOT)
Mobile technology devices may be school owned and might include: tablet, laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

- **The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies**

Use of digital and video images

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

- When using digital images, staff 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.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *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 unless explicitly agreed with the Headteacher in advance.
- 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 blog, particularly in association with photograph

- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the EU General Data Protection Regulation (GDPR) 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
- 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 transfer / 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.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff and Other Adults				Pupils			
	Allowed	Allowed at	Allowed for	Not Allowed	Allowed	Allowed at	Allowed with Staff permission	Not Allowed

		Certain Times	Selected Staff			Certain Times		
Mobile Phones may be brought in School	x							Handed in on entry
Use of Mobile Phone in Lessons				x				x
Use of Mobile Phone in Social Time		x						x
Taking Photos on Personal Devices				x				x
Use of Other mobile devices		x				x		
Use of personal email addresses in school		x						x
Use of School Email for Personal Emails				x				x
Use of Messaging Apps		x						x
Use of Social Media		x						x
Use of Blogs		x						x

When using communication technologies, the school considers the following as good practice:

- The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class email addresses may be used at KS1 and lower KS2, while pupils at Year 5 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies 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:

- Ensuring that personal information is not published
- Training is provided including: 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, parents / carers 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

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)				x		
On-line gaming (non-educational)					x	
On-line gambling					x	
On-line shopping / commerce					x	

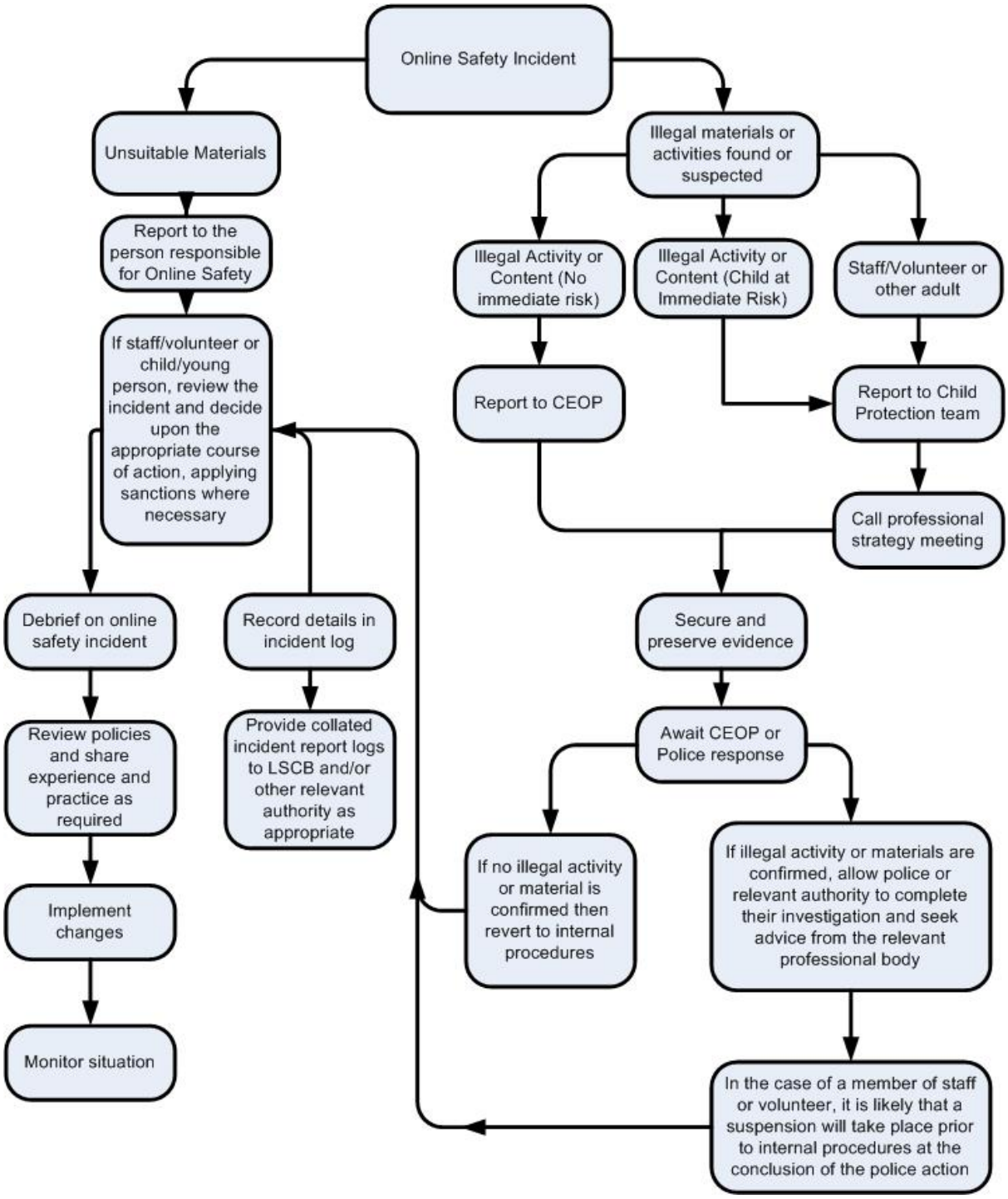
File sharing		x			
Use of social media			x		
Use of messaging apps			x		
Use of video broadcasting e.g. Youtube			x		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

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


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher	Refer to Deputy Headteacher	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 eg detention / exclusion
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							
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		x							
Unauthorised / inappropriate use of social media / messaging apps / personal email		x							
Unauthorised downloading or uploading of files		x							
Allowing others to access school network by sharing username and passwords			x						
Attempting to access or accessing the school network, using another student's / pupil's account			x						
Attempting to access or accessing the school network, using the account of a member of staff			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						
Continued infringements of the above, following previous warnings or sanctions			x			x	x		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			x						
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						
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							

Actions / Sanctions

Staff Incidents	Refer to Deputy Head	Refer to Headteacher Principal	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				
Inappropriate personal use of the internet / social media / personal email						x		
Unauthorised downloading or uploading of files	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		
Careless use of personal data e.g. holding or transferring data in an insecure manner		x				x		
Deliberate actions to breach data protection or network security rules		x						x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x		x				x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		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
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 / academy'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					x
Breaching copyright or licensing regulations	x					x		

Continued infringements of the above, following previous warnings or sanctions		x						x

Merridale Primary Primary School GDPR Privacy Notice Pupils and their Parents

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment and attainment information
- Medical information and details relating to Special Educational and/or disability needs
- Behaviour information (number/nature of incidents in which a pupil has been involved and consequences, including exclusions)
- Safeguarding information
- Photographs

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to carry out our legal obligations as a school
- to keep children safe
- to comply with the law regarding data sharing
- The lawful basis on which we use this information

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)
- We have obtained it as part of fulfilling a contract with you

We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Regulation 3 of the Education (Information About Individual Pupils) (England) Regulations 2013

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

The categories of parent information that the school collects, holds and shares includes the following:

- Contact information, including addresses, phone numbers and email addresses of parents and/or any other emergency contacts
- Financial information where appropriate, e.g. to check eligibility for FSM
- Information pertaining to home life where appropriate, e.g. where a pupil is identified as having a mental health issue or there are safeguarding concerns

Storing pupil data

- We hold pupil data for the duration of the child's educational journey with us.
- The school operates a records retention schedule that includes details on how long we keep information about pupils.
- We will only hold information to you for as long as necessary.
- How long we hold information will depend on the type of information.
- In accordance with GDPR, the school does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local authority
- the Department for Education (DfE)
- learning platforms and communication tools, including Teachers2Parents
- Our regulator Ofsted
- Suppliers and service providers
- Central and local government
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

Why we share pupil information

- We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
- We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
- We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DFE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, please contact dpo@merridaleprimary.co.uk or write to Merridale Primary School, Aspen Way, Wolverhampton WV3 0UP. Please address letters for the attention of the Data Protection Officer who will be able to provide the details for making a Subject Access Request.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact the data protection officer on dpo@merridaleprimary.co.uk or write to Merridale Primary School, Aspen Way, Wolverhampton WV3 0UP. Please address letters for the attention of the Data Protection Officer

Merridale Primary School GDPR Workforce Privacy Notice

The categories of school workforce information that we collect, process, hold and share include:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Photographs
- Data about your use of school's information and communications system
- Personal information (such as name, employee or teacher number, national insurance number)
- Special categories of data including characteristics information such as gender, age, ethnic group
- Contract information (such as start dates, hours worked, post, roles and salary information)
- Trade Union membership
- Health including any medical conditions and sickness records

Why we collect and use this information

We use school workforce data to:

- Enable you to be paid
- Facilitate safe recruitment as part of our safeguarding obligations towards pupil
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of the workforce data across the sector
- Support the work of the School Teachers' Review Body
- Enable the development of a comprehensive picture of the workforce and how it is deployed
- The lawful basis on which we process this information

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

We have legitimate interests in processing the data – for example, where:

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds that justify the school's use of your data.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment. Once your employment with us has ended we will retain this file and delete the information in it in accordance with our record retention schedule/records management policy.

Who we share this information with

We routinely share this information with:

- Our local authority
- The Department for Education (DfE)
- Your family or representatives
- Educators and examining bodies
- Our regulator Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for such as payroll
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our pupils with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education, including the data we share with them, go to:-

https://www.gov.uk/education/data-collection-and-censuses-for-schools

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data To contact the department: https://www.gov.uk/contact-dfe

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area we will do so in accordance with data protection law.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, please contact the data protection officer on dpo@merridaleprimary.co.uk or write to Merridale Primary School, Aspen Way, Wolverhampton WV3 0UP. Please address letters for the attention of the Data Protection Officer

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact the data protection officer on dpo@merridaleprimary.co.uk or write to Merridale Primary School, Aspen Way, Wolverhampton WV3 0UP. Please address letters for the attention of the Data Protection Officer