McMillan Nursery School

Online Safety Policy

2025-2026

Development of this policy

This online safety policy has been developed by:
Headteacher – Ms Cathy Stokes
Online Safety Champion – Miss Yasmin Shah

Schedule for Review

This Online safety policy was approved by the Governing Body on	26/11/25
The implementation of this policy will be monitored by	Cathy Stokes – Headteacher
Monitoring will take place	Termly
The Governing Body will receive a report of the implementation of the Online safety policy	Termly
The Online safety policy will be reviewed annually or more regularly in the light of new technologies, new threats to Online safety or incidents that have taken place. The next anticipated review date will be	September 2025
Should serious Online safety incidents take place, the following external persons and agencies should be informed, where appropriate	Filter.Education.BT.Lancshire Team LA Safeguarding Manager Police CEOP Internet Watch Foundation

McMillan Nursery School recognise the need to have procedures in place to ensure the online safety of the school community, including governors, staff and pupils and any other party that has access to its ICT systems, such as volunteers and students. The use of emergent technologies is supported both for use by staff and by pupils.

This policy applies to all members of the school community; staff, governing body, parents, students and volunteers, and to pupils who have access to and are users of school digital systems, both in and out of school.

AIMS

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction
- is published on the school website.

ROLES AND RESPONSIBILITIES:

HEADTEACHER

- has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding.
- responsible for ensuring that the Designated Safeguarding Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- will ensure that there is a system in place to allow for monitoring online safety.
- will receive regular monitoring reports from Educational Digital Services.
- will work with the responsible Governor, and IT service providers in all aspects of filtering and monitoring
- will be responsible for the development, maintenance and review of this policy
- will be responsible for keeping an online safety log

ONLINE SAFETY CHAMPIONS:

- will be responsible for the associated documents, such as image consents and acceptable use policies
- will liaise closely with Nursery school's Senior Designated Person where there is an issue relating to safeguarding
- Responsible for security and data management

GOVERORS

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
- The Governing Board members will receive regular information about online safety incidents and monitoring reports through termly Head Teacher reports.
- A member of the governing body will take on the role of Online Safety Governor to include:
    - regular meetings with the Designated Safeguarding Lead and Online Safety champion
    - checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
    - Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.
    - reporting to relevant governors meetings
    - Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

STAFF

- will be required to sign an Acceptable Use Policy to ensure the utmost professionalism with regard to online safety matters
- must ensure that all data relating to children held on computers, laptops (including those off site) and pen drives is protected by the use of secure passwords
- they immediately report any suspected misuse or problem to the Headteacher/DSL for investigation/action, in line with the school safeguarding procedures, in the absence of the headteacher – Deputy DSL
- all digital communications with parents/carers are on a professional level and only carried out using official school systems
- when children are using iPads – ensuring guided access is on, restricting children from using the internet.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media. i.e. do not accept friend requests or communications from learns or their family members (past or preset). If there is a preexisting relationship this should be discussed with the headteacher
- make use of home visits and professional conversations with parents to inform their understanding of a child's context with regards to technology within the home (e.g. how much and in what ways is tech used within the child's family?)

PARENTS

- Parents will be asked to sign an Acceptable Use Policy on behalf of their children covering the use of computers and other mobile devices which the children may use during the Nursery school day
- Parents will be encouraged to support Nursery in promoting good online safety practice and to follow guidelines set down by Nursery on the appropriate use of digital and video images which may be taken at school events
- Online safety information will be given to parents and will also be available on the nursery school website

IT SERVICE PROVIDER

McMillan Nursery school uses the Local Authority's technology service provided - Educational Digital Services. They

- maintain filtering and monitoring systems
- provide filtering and monitoring reports
- complete actions following concerns or checks to systems"

SECURITY AND DATA MANAGEMENT

In line with the requirements of the Data Protection Act 1998, sensitive and/or personal data held in Nursery school will be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection
- The main person responsible for the processing of data in Nursery is Miss. Shah (School Admin Officer)
- Data is usually stored on physical devices such as computers and iPads.
- Data from the server and workstation used in the office are backed up remotely under the RBUSS service with Educational Digital Services to protect business continuity.

USE OF MOBILE DEVICES:

- McMillan Nursery school makes use of iPads for the purpose of observing and assessing children
- Children have access to two iPads which are only used with adult directed activities to ensure close supervision.
- McMillan Nursery school does not permit the use of personal devices (by either governors, staff, volunteers, students or visitors) for use as a resource for teaching and learning
- Staff, students and volunteers may bring mobile phones and other mobile devices into Nursery for personal use but these should only be used before or after work and during lunchtime.
- Children are asked not to bring phones or tablets onto the premises
- Parents are asked not to use their mobile phones while within Nursery school grounds
- Mobile phones should not in any circumstances be used to take photographs of children, video them or capture any audio
- McMillan's Nursery school's Wi-Fi network address is hidden and cannot be seen by any personal mobile devices
- McMillan Nursery school does not have a mobile phone to use in the event of an emergency situation arising. If it is not possible to use Nursery's landline to make calls to parents in an emergency situation, staff will use their personal mobiles to contact parents

- Any concerns regarding the use of mobile devices being used in a manner which contravenes this policy should be brought to the attention of the Headteacher

USE OF DIGITAL MEDIA

- McMillan Nursery school acknowledges that photographs of children and staff may be considered as personal data in the terms of the Data Protection Act 1998
- McMillan Nursery School will seek written consent from parents, guardians or carers for photographs and video clips of children to be taken and used
- It is Nursery school's policy to delete any photographs and video clips of children which are stored on any computer or device once that child has left Nursery
- Photographs of children are used in Learning Journeys, displays in Nursery, and on Nursery school's website. Children will not be identified by name where their image is on the website
- Every effort will be made when photographing children for Learning Journeys to capture images of individual children only. However, in practice, there are likely to be situations where a group of children are photographed together undertaking a group activity. Written consent will be sought from parents for permission to use any such group photographs
- Staff will be informed where consent is not given for the use of photographs of any particular child.
- Staff will endeavour to ensure that all images captured do not show children either distressed or injured or in any context which could be deemed embarrassing or open to any misinterpretation.

PARENTS TAKING PHOTOGRAPHS / VIDEO:

- Parents are entitled to take photographs of their own children provided these images are for their own personal use. Photographs which include images of other children or which are taken for purposes other than personal use could constitute a breach of Data Protection legislation.
- Parents are reminded that Nursery strongly discourages the publishing of photographs taken at Nursery on social networking sites.
- Permission should be sought to take photographs or video which will include images of children other than parents' own children.

STORAGE OF PHOTOGRAPHS / VIDEO:

- Photographs are stored on school devices, including the server, workstation, laptops and iPads.
- All school devices are password protected
- Taking personal photographs with school equipment is not permitted.

- Staff are responsible for deleting photographs of children who have left the setting from the devices they use / their folder on the laptops .

COMMUNICATION TECHNOLOGIES

Email:

- All members of staff will have an email address in the format (name)@mcmillan.lancs.sch.uk which should be used for all work communications. Work email addresses should not be used for any personal communications.
- Pupils will not be assigned an email address.
- Parents should only be contacted via work email accounts (and not via personal email accounts).
- Emails are covered by The Data Protection Act (1988) and the Freedom of Information Act (2000); therefore safe practice should be followed in terms of record keeping and security.
- Emails may be monitored at any time in accordance with Nursery school's Acceptable Use Policy
- Email users should notify the Head Teacher if they receive any email which makes them uncomfortable, which is offensive, threatening or bullying in nature
- Email users should not open attachments which they suspect may contain illegal content (as they might then inadvertently be committing a criminal act)
- Emails should be set up (via options / layout / email signature) with the following disclaimer: This email and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent McMillan Nursery School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this email or its contents. If you have received this email in error, please contact the sender. Please note that email may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000

Social Networks:

At the current time, the Nursery does not have its own page on a social networking site.

- Children do not access social networking sites.
- Staff must be aware that they must not disclose any information through any social networking site, relating to the nursery, nursery staff or users of the nursery.
- Children or parents will not be added 'as friends' on any social network i.e. Facebook .

Instant Messaging or VOIP (voice over internet protocol)

- The use of Nursery School iPads for real time communication such as FaceTime is not permitted
- At the current time, McMillan Nursery School does not make use of any text messaging service to message parents.

Virtual Learning Environment

- McMillan Nursery School uses an Online Learning Journal 'Tapestry'.

Parents and staff have secure access. Parents sign a parental agreement which ensures safe use of 'Tapestry'.

WEBSITE

- McMillan Nursery School's website should comply with the requirements of the School Information (England) (Amendment) Regulations 2014 by making certain information publicly available
- McMillan Nursery School's website is updated by Miss. Stokes and Miss. Shah

The admin function is password protected

- No child should be identified by name on the Nursery School website
- All staff are aware that photos may only be published onto the website following permission sought from parents. No personal details will be attached to photos.
- The school admin officer and head teacher update the school website and ensures the content is relevant and current.
- All downloadable materials will be in a read-only format (PDF), to prevent content being manipulated and potentially re distributed without the schools' consent.

INFRASTRUTURE AND TECHNOLOGY

- McMillan Nursery School is responsible for ensuring that the school network is as safe and secure as is reasonably possible
- McMillan Nursery School has a Service Level Agreement with Educational Digital Services (EDS) to provide broadband, email, filtering and anti-virus services, together with SIMS support and daily remote backup.
- Internet access is filtered for all users.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- McMillan Nursery School has Sophos Anti-Virus software as part of its package of support from EDS.
- Internet access is filtered for all users via Lightspeed, provided as part of the agreement with EDS
- Servers, wireless systems and cabling must be securely located and physical access restricted. They are stored in a high locked comms cabinet in the school office.
- McMillan Nursery School has a Service Level Agreement with EasyTech to provide ongoing ICT support
- Master / administrator passwords are kept securely locked away
- Access to McMillan Nursery School's Management Information System (SIMS) is restricted to the Headteacher and the School Admin Officer
- Children have access to two iPads in Nursery at the current time which are only used with guided access. Nursery intends to increase the number of portable devices available to children as funding permits.
- McMillan Nursery School's Wi-Fi network is password protected and available for use only by Nursery's portable devices. The network is managed by Easytech
- McMillan Nursery School works with Easytech to ensure that all appropriate licenses are held for any software used
- Software is installed onto devices only by Easytech
- The Service Level Agreement with Easytech allows them to install updates on all portable devices, laptops and computers to which children have access.

Routine updates, critical updates and patches for McMillan Nursery School's server and workstation in the office are managed by Miss Shah in accordance with advice and assistance from EDS

- McMillan Nursery School provides a laptop for its teachers to use at home. These are password protected. Personal use of this equipment is not permitted.
- It is Nursery School's policy that remote laptops are brought on to site at regular intervals (termly) to allow up to date anti-virus software to be installed.
- Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of the Headteacher and online safety governor.

Filtering

- the school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by Education Digital Services by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- filtering logs are regularly reviewed by educational digital services and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

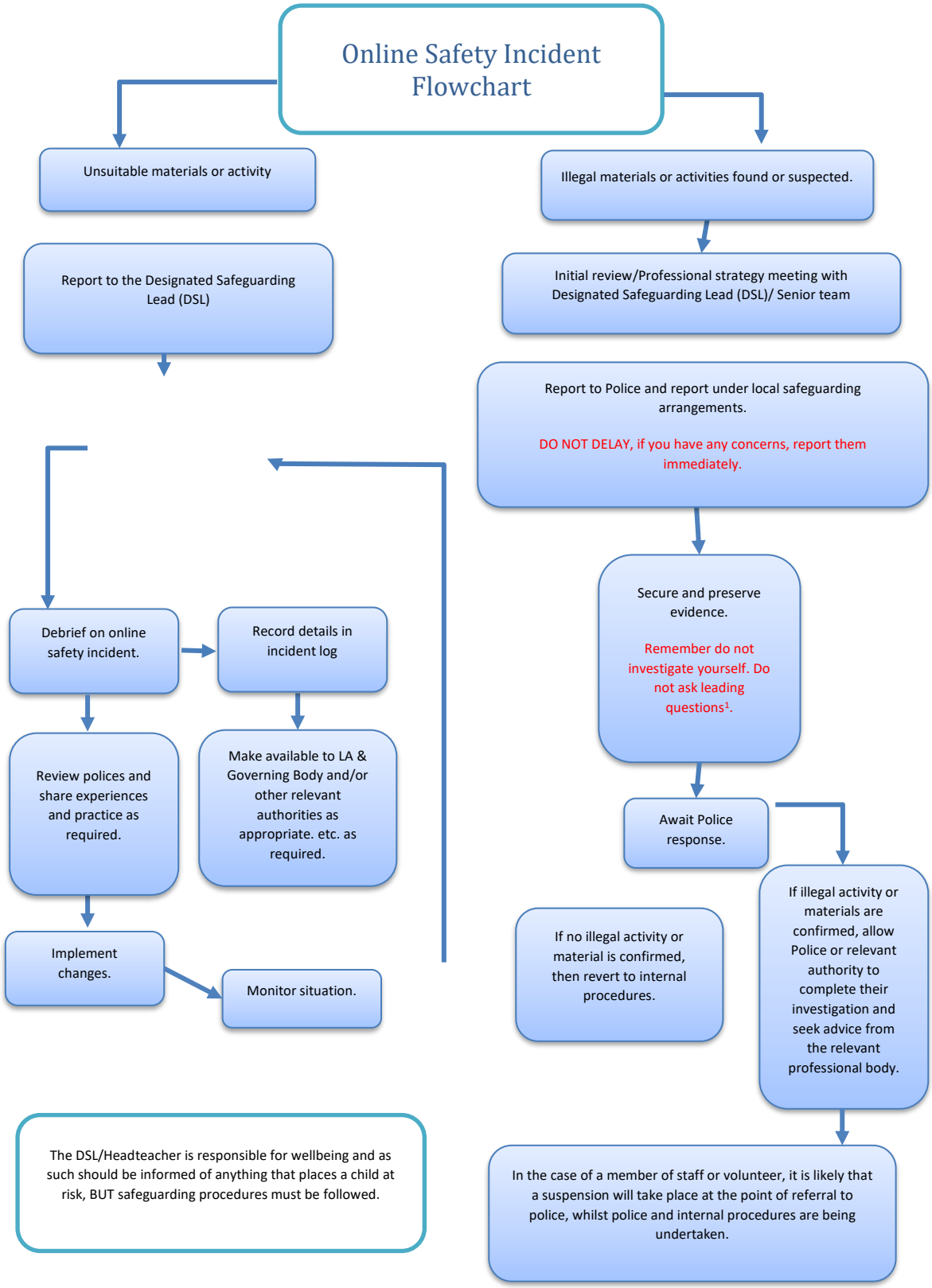
- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

DEALING WITH INCIDENTS

- The headteacher will ensure that an online safety log is maintained. Reports on any online safety incidents arising will be made termly to the Governing Body
- Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation.

- It is imperative that any suspected illegal activity is not investigated personally; instead the appropriate authorities must be brought in to investigate. This is to protect staff from potentially committing an illegal offence. Potential illegal content will always be reported to the Internet Watch Foundation (http://www.iwf.org.uk). Staff must never try to investigate the incident themselves.
- Illegal offences could be:
    - Accessing child sexual abuse images
    - Accessing non-photographic child sexual abuse images
    - Accessing criminally obscene adult content
    - Incitement to racial hatred
- 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 Flowchart



DEALING WITH INAPPROPRIATE MISUSE

Examples of such and procedure and sanctions are listed below

Incident	Procedure and Sanctions
Accidental access to inappropriate materials	• Minimise webpage / turn off monitor • Inform Headteacher/DSL • Complete incident log • Report to EDS Lightspeed filtering team if necessary • Consider disciplinary action if a persistent "accidental" offender
Malicious use of logins or passwords other than own	• Inform Headteacher • Complete the incident log • Consider disciplinary action • Involve third parties where appropriate
Deliberate searching for inappropriate materials	
Bringing inappropriate electronic files from home	

• 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 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 or national / local organisation (as relevant).

- Police involvement and/or action

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

incidents of 'grooming' behaviour

- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

• Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

SCHOOL ACTIONS AND 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.

ACCEPTABLE USE and BEHAVIOUR POLICY (AUP)

• An AUP is intended to ensure that all users of technology within school are responsible and protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes

• AUPs are required for staff, children and visitors/guests and should be completed before any use of technology in Nursery is permitted. In practice, parents will sign the AUP on behalf of their children

• A list will be kept of any children who are, for any reason, not allowed to access technology in Nursery. Staff will be made aware of any children this affects

EDUCATION AND TRAINING

- McMillan Nursery School is committed to teaching staff and children to be digitally literate and aware of how technology can be used
- McMillan Nursery School acknowledges that OFSTED require schools to be aware of three main areas of online safety risk, namely

  - Content

  McMillan Nursery School will endeavour to ensure that the internet is not accessible by children when using iPads during the Nursery School day. Children are given access to apps, such as games but under guided access. It is possible that children may inadvertently access the internet, but EDS Lightspeed filtering should block inadvertent access to any inappropriate content.

  - Contact

  McMillan Nursery School acknowledges that children need to learn appropriate conduct when accessing digital technologies. In practice, in our Nursery School setting, there is very minimal risk of circumstances arising which would enable grooming, cyber bullying or identity theft to take place

  - Conduct

  McMillan Nursery School is committed to teaching children that access to digital technologies should be restricted. We would always try to encourage children to participate in a range of activities rather than spend the whole session using iPads. This is the start of a process of educating children about appropriate conduct using technology

  Commerce

  McMillan Nursery School teach age-appropriate online risks to children. i.e. Tell an adult

Review: Autumn 2026