Meadlands Primary School

Online Safety Policy

Status	Non-statutory
Review cycle	Annual
Date written/last reviewed	September 2025
Date of next review	September 2026
Headteacher	Mrs Wreford
Chair of Governors	Christina Powell and Melissa Shaw
Published on website	Yes

Introduction

This policy is part of the School's Statutory Safeguarding Policy and Staff Code of Conduct. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes. The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Relationships, Communication and Behaviour Policy, PSHE, Computing policy, Mobile Phone Policy, X Policy and Acceptable Use Policy).

- The online safety policy will be reviewed when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy, and it has been agreed by the SLT and shared with Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Meadlands Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying referring also to our Relationships, Communication and Behaviour Policy and Safeguarding and Child Protection Policy
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Sexting
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of our community (including staff, pupils/pupils, volunteers, parents/carers, governors, visitors, community users) who have access to and are users of our IT systems, both in and out of Meadlands Primary School.

Roles and responsibilities

Role	Key Responsibilities
Headteacher: Jo Wreford Deputy Headteacher: Laura Tadman-Barson School Business Manager: Jolene Gee	• Headteacher to be trained up to Level 3 Safeguarding • To take overall responsibility for online safety provision • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure annual radicalisation updates and suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the IT Technician (Helen Frank) • To receive an annual report from the DPO following a GDPR audit • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.

Designated Safeguarding Lead DSL (also Headteacher): Mrs Jo Wreford Deputy DSLs: Jolene Gee Sue Kelly	• To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • To have oversight of the filtering and monitoring processes. • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as safeguarding incidents. • Facilitate training and update annual regarding Safeguarding advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.

Safeguarding governor (including online safety): Komal Parekh	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety Governor will include: regular review with the Designated Safeguarding Lead
Computing Lead: Sarah Taunton	• To oversee the delivery of the online safety element of the Computing curriculum
IT technician: Helen Frank	• To report online safety related issues that come to their attention, to the Designated Safeguarding Lead, Computing Lead and where appropriate the Data Protection Officer. • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) through Sophos and LGFL - access controls/encryption exist to protect personal and sensitive information held on school-owned devices (Bitlocker). - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology, online platforms including filtering systems are monitored weekly through LGFL reports and that any misuse/attempted misuse is reported to the Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place. • To keep up-to-date documentation of the school's online security and technical procedures
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Role	Key Responsibilities
All staff, volunteers and contractors	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by all staff annually • To report any suspected misuse or problem to the appropriate person. • To maintain an awareness of current safeguarding and online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology Exit strategy • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving Usernames, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset. Please refer to the Off-boarding flowchart.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren. • To consult with the school if they have any concerns about their children's use of technology • To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology including social media.
Data Protection Officer:	• To advise and inform the school and its staff about their obligations to comply with GDPR and any other data protection legislation • To monitor the school's compliance with GDPR, train staff, conduct audits etc. • To be the first point of contact with the ICO and data subjects

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be published on the school website
- Policy to be part of school induction pack for new staff.
- Annual training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school and signed by both the pupil and parent.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Designated Safeguarding Lead via CPOMs.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complainant is referred to the Chair of Governors and the DO (Designated Officer).

Pupil online safety Education and Curriculum

This school:

- Has a clear, progressive online safety education programme as part of the Computing, PSHE and SRSE curriculum. This covers a range of skills and behaviours appropriate to their age and experience.
- Plans online use carefully, to ensure that it is age-appropriate, and supports the learning objectives for specific curriculum areas.
- Will remind pupils about their responsibilities through the pupil Acceptable Use Agreement(s).
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.

-

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program.
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- Runs a rolling programme of online safety advice, guidance and training for parents. Through our Meet the Teacher event we will share that Meadlands uses LGFL to filter and monitor online use along with what children will be expected to do online as part of their learning.

Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements.
- understand the significance of misuse or access to inappropriate materials and are aware ofthe consequences.
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so.
- understand the importance of adopting good online safety practice when using digital technologies in and out of school.
- know and understand school policies on the use of mobile and hand-held devices including cameras, staff, volunteers and contractors.
- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

Parents/Carers

- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions.
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues.
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school.
-

Managing the IT Infrastructure (please review the school's internal Information Security policy)
Data security: Management Information System access and Data transfer (please review the school's internal Information Security policy)

Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices or hand-held device.
- No pupils unless Year 6, or Year 5 summer term, should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be securely in the classroom and returned at the end of the day.
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off as per the Mobile Phone policy.
- No images or videos should be taken on mobile devices apart from the Headteacher's Deputy Headteacher's and School Business Manager's mobile phone and the school's mobile phones.
- All visitors are requested to turn their phones off when they enter the premises.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone.
- Staff may use their phones during break times and in the staff room. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

Storage, Synching and Access

The device is accessed with a school owned account

- The device (IPADS, Dell and HP laptops and Chrome Books) has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.
- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Staff use of personal devices

- Any permitted images or files taken in school on a personal camera must be downloaded and deleted

from the device in school before the end of the day.

- Staff will be issued with a school phone where contact with-parents or carers is required, for instance for off- site activities including longer residential trips.
- Mobile Phones and personally-owned devices will be switched off. The exceptions to this are: the safeguarding team who need to access CPOMS via mobile double authentication. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and then report the incident to the Headteacher and DPO.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually).
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- Since the implementation of GDPR 2018, the school has chosen not to act retrospectively. From this point forward the school will obtain permission for the use of images to remain on the school website and other media outlets including social media for a period of 5 years.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.