MANOR LEAS INFANT SCHOOL

Learning for Life

Online Safety & Acceptable Use Policy

Policy number	63
Policy revision	10
Policy reviewed	Autumn 2024
Review date	Autumn 2025
Committee	FB
Author	Computing Lead

1. Aims

Our school aims to:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees

Identify and support groups of pupils that are potentially at greater risk of harm online than others

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

[Relationships and sex education – remove if not applicable, see section 4]

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

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

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The trustee board

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

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

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

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

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

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

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

All trustees will:

- Ensure they have read and understand this policy
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The headteacher

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

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) [and deputy/deputies] are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school Working with the trustee board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on cpoms and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on cpoms and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 2 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the headteacher and/or trustee board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- This list is not intended to be exhaustive.

Please note that all use of ICT in school may be subject to monitoring. This includes, but is not limited to, email, telephone conversations, electronic messaging, internet use, and system access.

Monitoring is used by the school for the following purposes:

- To maintain and ensure security of systems and information;
- To check for unauthorised use;
- To establish facts relevant to school business;
- To ensure quality assurance and ensure that procedures are being followed;
- To undertake disciplinary, performance, and capability proceedings; and
- To prevent or detect crime.

3.4 The Computing Lead

The Computing Lead will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use;
- Review this policy regularly and bring any matters to the attention of the headteacher;
- Advise the headteacher and the board of trustees on all online safety matters;
- Engage with parents and the school community on online safety matters at school and/or at home;
- Liaise with the local authority, ICT technical support and other agencies as required;
- Retain responsibility for reviewing the online safety incident records on cpoms;
- Make themselves aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function and liaise with the headteacher and the responsible trustee to decide on what reports may be appropriate for viewing.

3.5 ICT Technical Support Staff

Technical support staff are responsible for ensuring that the ICT technical infrastructure is secure; this will include as a minimum:

- Anti-virus is fit for purpose, up-to-date and applied to all capable devices;
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate;
- Any online safety technical solutions such as internet filtering are operating correctly;
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and headteacher;
- Passwords are applied correctly to all users regardless of age;
- The IT system administrator password is to be changed on a monthly (30 day) basis.

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for maintaining an understanding of this policy and implementing this policy consistently. If anything is not understood, it should be brought to the attention of the headteacher;

Staff agree to:

Passwords and security

- Protect their username and password from misuse and not share their username or password with others. Passwords should be recorded unless it is done so securely and you are the only one who can access is it.
- Change their passwords regularly and ensure it is not easily guessable; Passwords must be minimum 8 characters in length and include a mixture of upper/lowercase, numbers and special characters.
- Change their default password and not use the same password across different accounts (work and private) and/or applications.
- Not allow unauthorised persons to use their work device
- Operate a clear screen policy when a device is unattended e.g. engaging the lock screen
- Not introduce unauthorised software, hardware or removable media on work devices without permission from the Headteacher or Data Protection Officer (Heather Brunsden)
- Not introduce removable media to school ICT without permission from the headteacher or Heather Brunsden, Data Protection Officer as it may contain malware designed to harm school systems.
- Ensure all ICT is returned to school when no longer required. This is to ensure devices are securely wiped or destroyed.
- Only access or attempt to access ICT that you have been authorised to access or attempt to access information for official school purposes aligned with your role and this must be on a need to know basis.
- Not break copyright or carry out any activity that negatively impacts intellectual property rights.
- Prevent inadvertent disclosure of information and avoid being overlooked when working off school premises
- Know that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing The Headteacher (DSL) or the Data Protection Officer (Heather Brunsden)
- Follow the correct procedures by contacting F1 if they need to bypass the filtering and monitoring systems for educational purposes
- Report all security incidents and suspected security incidents in accordance with the school's Security Incident Policy to Heather Brunsden, Data Protection Officer. If you identify suspicious activity while using ICT or believe that you are the victim of malware e.g. a virus you must stop what you are doing, power off your ICT and report it immediately.
- Work with the DSL or deputies to ensure that any online safety incidents are logged on cpoms and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of ‘it could happen here’
- Not use personal mobile devices in school in the presence of pupils, unless in exceptional circumstances and when permission has been granted by the headteacher
- Only use school devices to take images of pupils for legitimate purposes

Emails

- Take care when opening an attachment or clicking on any link within any email unless you are confident the email is legitimate.
- Only send emails from their own authorised account and not using personally owned email
- Check the recipients of e-mail are correct to avoid accidental release to unintended recipients. Particular care must be taken when using auto complete in your email client as an unintended email address may be used in error.
- Delete suspicious emails and not forward them to other recipients. If you suspect an email contains malware please contact F1 Group, 01522 508080.
- When sending an email to more than one recipient and it is necessary to protect email addresses, the blind carbon copy (BCC) feature must be used.
- When sending sensitive information via email ensuring it is done so securely.
- Only delegating access to email accounts following a clear business need and only when authority is provided by the email account owner, or in their absence, the Head Teacher. To arrange delegate access please contact Heather Brunsden, Data Protection Officer. Delegate access must not be provided by supplying details of a User's credentials i.e. username and password. When provided with delegate access the person accessing emails must take reasonable precautions to avoid opening private emails. If it becomes readily apparent that an email is of a personal nature the reader must not open it or stop immediately if the email has been opened.

Portable and personal devices

- Ensure that all portable ICT used to store or process sensitive information, such as personal data, is encrypted.
- Only remove ICT from school premises when there is a clear business need.
- Protect portable devices when off the school premises e.g keeping them under lock and key and not leaving them in a car overnight Only removing ICT from school premises when there is a clear business need.
- Connect portable devices to the school's ICT network on at least a monthly basis in order to receive security updates. You must ensure devices remain connected until such time updates have been received and applied i.e. Windows updates.
- School recommends that only work devices are used to access school data. If a personal device is used to access school data, school recommends that staff install anti-virus software.

Activity

- Not process materials, accessing websites or posting comments that could be construed as racist, sexist, defamatory, offensive, obscene, illegal or otherwise inappropriate material.
- Not carry out illegal, fraudulent or malicious activity.
- Not use personal accounts to conduct school business or to transmit or receive school information.
- Not use school ICT to carry out or support business which is unrelated to the school.
- Ensure any personal use of the internet is reasonable, proportionate and occasional and must not interfere with the performance of your role or the performance of the system.
- Only use pupil images when authorised by parents
- Only give permission to pupils to communicate online with trusted users

This list is not intended to be exhaustive.

3.7 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

➢ What are the issues? – UK Safer Internet Centre

➢ Hot topics – Childnet

➢ Parent resource sheet – Childnet

3.8 Pupils

Pupils are expected to:

- Follow the terms on acceptable use of the school's ICT systems and internet

3.9 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and are expected to read and follow it.

4. Educating pupils about online safety

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

All schools have to teach:

Relationships education and health education in primary schools

Primary schools insert:

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

Use technology safely and respectfully, keeping personal information private

Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

The safe use of social media and the internet will also be covered in other subjects where relevant. We promote the STOP-CLOSE-TELL approach to support pupils to know what to do if they have a concern about the technology they are using.

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

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or ClassDojo as appropriate. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings if appropriate.

The school website lets parents/carers know:

What systems the school uses to filter and monitor online use

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

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

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

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils in assemblies or in Computing lessons, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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

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

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

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

6.3 Examining electronic devices

The headteacher or assistant headteacher in her absence, can confiscate any electronic device that they have reasonable grounds for suspecting:

Poses a risk to staff or pupils, and/or

Is evidence in relation to an offence

If pupil has a device on their person and will not give it to a member of staff when asked, parents/carers of the child will be contacted and asked to collect the device.

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

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

Cause harm, and/or

Undermine the safe environment of the school or disrupt teaching, and/or

Commit an offence

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

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the

material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

The pupil and/or the parent/carer refuses to delete the material themselves

7. Acceptable use of the internet in school

Parents/carers are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 1) on behalf of their child. Staff, volunteers and trustees are expected to sign to say they have read and understood the ICT Acceptable Use Policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

We will monitor the websites visited by pupils, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

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

8. Pupils using mobile devices in school

Pupils may not bring mobile devices into school. If a pupil brings a mobile device into school, it will be confiscated and given to the pupil's parent/carer at the end of the day. If pupil has a device on their person and will not give it to a member of staff when asked, parents/carers of the child will be contacted and asked to collect the device.

9. How the school will respond to issues of misuse

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

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

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

10. Social Media

10.1 Staff responsible for the school's social media accounts will delete as soon as reasonably possible:

Abusive, racist, sexist, homophobic or inflammatory comments

Comments we consider to be spam

Personal information, such as telephone numbers, address details, etc.

Posts that advertise commercial activity or ask for donations

Every reasonable effort will be taken to politely address concerns or behaviour of individual users. If users are repeatedly abusive or inappropriate, they will be blocked.

Staff responsible for our social media accounts will also ensure that all content shared on social media platforms is age appropriate for the school community.

10.2 Following other social media users

The school:

May 'like' Facebook pages with a non-commercial interest – being 'liked' by us doesn't imply endorsement of any kind

May follow other users if you follow us on X (formerly Twitter) – being followed by us doesn't imply endorsement of any kind

10.3. Personal use of social media by staff

The school expects all staff (including trustees and volunteers) to consider the safety of pupils and the risks (reputational and financial) to the school when using social media channels, including when doing so in a personal capacity. Staff are also responsible for checking and maintaining appropriate privacy and security settings of their personal social media accounts. Colleagues who are considering social media campaigns should firstly consult the headteacher for guidance.

Staff members will report any safeguarding issues they become aware of.

When using social media, staff **must not**:

- Use personal accounts to conduct school business
- Accept 'friend requests' from, or communicate with, pupils past or present if they are under 18 years old
- Complain or post negative or offensive comments about the school, individual pupils, colleagues, trustees or parents/carers
- Reference or share information about individual pupils, colleagues or parents/carers
- Post images of pupils
- Express personal views or opinions that could be interpreted as those of the school
- Link their social media profile to their work email account
- Use personal social media during timetabled teaching time except in a professional capacity
- Engage in activities on the internet that might bring the school into disrepute.

Any concerns regarding a member of staff's personal use of social media will be dealt with in line with the staff behaviour policy.

Any communication received from current pupils (unless they are family members) on any personal social media accounts will be reported to the designated safeguarding lead (DSL) or member of the senior leadership team immediately.

Staff should also not also have contact via personal accounts with past pupils if they are under 18 years old (if ongoing communication is required, this should be using via official school channels).

10.4 Personal use of social media by parents/carers

The school expects parents/carers to help us model safe, responsible and appropriate social media use for our pupils.

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, parents and carers should:

Be respectful towards, and about, members of staff and the school at all times

Be respectful of, and about, other parents/carers and other pupils and children

Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

Parents/carers **should not** use social media to:

Complain about individual members of staff, other parents/carers or pupils

Complain about the school

Make inappropriate comments about members of staff, other parents/carers or pupils

Draw attention to, or discuss, behaviour incidents

Post images of children other than their own

11. Training

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

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

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

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

Abusive, threatening, harassing and misogynistic messages

Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

Develop better awareness to assist in spotting the signs and symptoms of online abuse

Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake yearly child protection and safeguarding training following the Lincolnshire 6 Year Pathway, which will include online safety. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

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

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on Cpoms.

This policy will be reviewed every three years by the trustee board.

14. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

ICT and internet acceptable use policy

Mobile Technology Policy

Parent Code of Conduct

Staff Code of Conduct

Security Incident Policy

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

Rules for Responsible Internet Use

We use the school computers and the Internet to help us learn.

These rules will help us to stay safe and be fair to everyone.

Please read through the following rules with your child(ren)

- I agree to follow the internet safety rules whenever I go online at school;
- I will always ask a member of staff before using the internet;
- I will only use my school login details and password;
- I will keep my login details private;
- I will only use the websites that my teacher tells me I can;
- I will only email people my teacher has said I can;
- I will make sure any messages I send are polite and sensible;
- I will never give my home address, phone number or full name over the internet;
- I will tell an adult straight away if I come across something that makes me feel uncomfortable (remember the Stop-Close-Tell rule – stop what I am doing, close the device and tell an adult)
- I know who to ask if I need help;
- I must ask my teacher before I print so that I do not waste paper and ink;
- I understand that the school may check my computer files and the internet sites I visit;
- I understand that if I do not follow these rules I may not be allowed to use the internet or computer.

Appendix 2: online safety training needs – self-audit for staff

Adapt this form to suit your needs.

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, trustees and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	