



Online Safety Policy

Policy reviewed: Autumn 2023

Date of next review: Autumn 2024

The Online Safety Policy relates to other policies including those for Anti-bullying, Safeguarding and Child Protection, Acceptable Use policy and the Staff Code of Conduct.

Manby Lodge has a Computing Leader, Miss Lonergan who works in collaboration with The Designated Safeguard Leader (DSL), and PSHE Leader, in order to ensure this policy meets the ever-changing issues relating to the Internet and its safe use.

Our Online Safety Policy has been written, building on best practice and government guidance.

Keeping Children Safe in Education (KCSIE) 2022 recognises that school staff have a duty to keep children safe online and to teach them how to use the internet safely. Please refer to our school's Safeguarding and Child Protection Policy for further information.

1. Introduction and Overview

Review and Monitoring

Our Online Safety Policy will be reviewed annually **or** when any significant changes occur with regard to the technologies in use within the school

What is Online safety?

Online safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. Online safety highlights the need to educate children about the benefits and risks of using internet technologies and electronic communications and provides safeguards and awareness for users to enable them to control their online experience.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Manby Lodge Infant School with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.

- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying, in line with the school's Behaviour / anti-bullying policy and Safeguarding 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.

Rationale

- The risks to pupils online could include: exposure to inappropriate content, promotion of harmful behaviours, hate content, inaccurate or illegal material, grooming and sexual exploitation, exposure to radicalisation, online bullying, lack of awareness of a digital footprint, identity theft, breach of copyright, invasion of privacy and sharing of private content.

Communication

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

- Policy to be posted on the school website and available to all members of the school community.
- All staff or visitors must read and sign the 'Acceptable Use Policy' before using any school technology resource
- Regular updates and training on online safety for all staff, including any revisions to the policy

2. Education and Curriculum

Pupil online safety curriculum

- Manby Lodge has a clear, progressive online safety education programme as part of the Computing, PSHE (Jigsaw) and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience. PADDY the school's Online Safety mascot will continue to underpin the key behaviours for staying safe online.
- Pupils will be taught to evaluate internet content for authenticity and to be critical of its contents
- Pupils will be shown how to publish and present information appropriately to a wider audience
- Pupils will be taught how to report unpleasant internet content
- Pupils will understand that information put online leaves a digital footprint or trail.
- Pupils will understand how we should talk to others in an online situation.
- Pupils to gain knowledge and understanding about sharing more globally on the Internet.

- Pupils will be able to identify the steps that can be taken to keep personal data and hardware secure.
- Online safety will be reinforced across the curriculum when children use the internet to enhance their learning

Introducing the Online Safety policy to pupils

- Appropriate elements of the Online Safety Policy will be shared with pupils through our online safety curriculum work and through use of PADDY within the classrooms
- PADDY safety posters will be in all classrooms and inside the laptop trolleys
- Pupils will be informed that network and internet use will be monitored
- Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for pupils, for example, Anti-bullying Week and Internet Safety Day.

Staff and the Online Safety policy

- All staff will have access to the School Online Safety policy and its importance explained
- Regular updates and training on online safety shall be provided for all staff, including any revisions to the policy
- The school 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 etc.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the school Online Safety policy in newsletters, Dear Parents and on the school website
- Internet issues will be handled sensitively to inform parents without undue alarm
- A partnership approach with parents will be encouraged. Where possible we will endeavour to hold a workshop for parents annually. We will focus on strategies that ensure that as many parents as possible attend this.
- The school will ask all new parents to sign the parent agreement when they register their child with the school.

3. Incident management

- There is strict monitoring and application of the online safety policy, including the Acceptable Use Policy and a differentiated and appropriate range of sanctions
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school
- Any concerns about staff misuse must be referred to the Head teacher, in line with the school's Whistleblowing Policy
- Concerns of a child protection nature must be referred to one of the DSLs via CPOMs, unless the concern is about the Head teacher in which case the concern is referred to the Chair of Governors
- Staff, pupils, volunteers and parents will be informed of the online safety concerns procedure
- The Police will be contacted if one of our staff receives online communication that we consider is particularly disturbing or breaks the law
- We will immediately refer any suspected illegal material to the appropriate authorities and inform the L.A.

4. Managing IT and Communication Systems

Managing internet access and filtering

- The school's internet access is provided by RM and includes filtering appropriate to the age of pupils, in according with DfE guidelines. The school will work in partnership with RM to ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable and updated as necessary.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and inter-linked online content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor EAC (our school's IT support provider) can accept liability for the material accessed, or any consequences of internet access.
- Virus protection will be updated regularly
- If staff or pupils come across unsuitable online materials, the source/website must be reported to one of the DSLs via CPOMs.

E-mail

Manby Lodge:

- Provides staff with an email account for their professional use, and should use personal email addresses through a separate account
- We will also use anonymous e-mail addresses, for example head@, office@
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

- Will ensure that email accounts are maintained and up to date

Staff email

- Staff will use LA- or school-provisioned e-mail systems for professional purposes
- Never use email to transfer staff or pupil personal data unless it is protected with secure encryption through Egress Switch when emailing outside of the school

Authorising internet access

- All staff must read and sign the '**Acceptable Use Policy**' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems
- Parents will be asked to sign and return a consent form.

5. Digital Content

Published content and the school web site

- The school website will comply with the statutory DfE requirements
- The contact details on the school website and other public sites should be the school address, e-mail and telephone number. Staff or pupil's personal information will not be published.
- The School Business Manager, Helen Plummer, will take overall editorial responsibility and ensure that the school's website and other related public content is accurate and appropriate.
- The school will seek to ensure that the use of internet-derived materials by staff and by pupils complies with copyright law.

Publishing photographs, images and work

- Written permission from parents or carers will be obtained before photographs or video of pupils are published
- Photographs that include pupils will be selected carefully.
- Pupils' full names or personal information will not be used on the school website or other public sites
- Parents should be clearly informed of the school policy on publishing images, both on school and independent electronic stores.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The school will audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

6. Data Security and equipment

- Management information system access, storage and data transfer will comply with the Data Protection Act.
- Permission needs to be sought from the Head teacher for school devices to be taken off the school premises. No encryption-level data will be stored on non school-based external devices. The school will provide encrypted storage devices for sensitive data.
- Devices from home should not be used at school unless permission has been given from the Head teacher.
- Staff will have regular Cyber Safety training. Staff are guided to report Cyber threats via our School Business Manager to the [website Action Fraud](#).

Social networking and personal publishing

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.



Acceptable Online Usage and Permission

Parent/guardian name

Pupil name:

Pupil's class:

Part 1)

ICT and the related technologies such as the Internet are an expected part of children's daily learning in school. The following is designed to ensure that all parents/ guardians are aware of their responsibilities when using the internet with their children. Parents/ guardians are expected to sign this form and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher or ICT leader.

I, the parent / carer, am aware of the pros and cons of my child using the internet. I will support the school's E-safety policy and help my child to be safe and responsible in their use of ICT and related technologies. I will promote E-safety with my child and will help them to develop a responsible attitude to system use, communications and publishing.

For example:

- I will encourage my child not to share personal information e.g. address and telephone number with people online.
- I will encourage my child not to use inappropriate language and to be polite and friendly when using the internet
- I understand that all my/my child's use of the internet is monitored and logged when using school software

I will report any incidents to the school that may breach this policy.

I agree to follow this code of conduct and to support the safe use of ICT with my child.

Part 2)

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and other digital technology, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered service and teaching online-safety skills to children.

Parent's signature:..... Date: