Manor Park

Primary School

Online Safety and Acceptable Use Policy

Date of Last Review: June 2021

Frequency of Review: Annually

Date of Next Review: June 2022

Designated Senior Person for Child Protection: Jill O'Connor Headteacher

Deputy Designated Senior Person for Child Protection: Deb Perkins Lead Learning mentor

Named Governor for Safeguarding & Child Protection: Richard Drudge

Local Authority Designated Officer (LADO), for allegations against staff: David Stanfield at LADO@coventry.gov.uk Tel: 02476 978499

Chair of Governors: Sarah Leigh
Email: s_leigh@manorpark.coventry.sch.uk

Vice-Chair of Governors: Matthew Potts
Email: m_potts@manorpark.coventry.sch.uk

MANOR PARK PRIMARY SCHOOL
Online Safety Policy

This online safety policy will be used in conjunction with the following policies and documents:
Child Protection and Safeguarding Children, Data Protection, Social Media, Digital Recording, Mobile Phones and Use of Social Media, Anti-bullying, Code of Professional Conduct, curriculum plans, and home-school acceptable use agreements.

Manor Park Online Computing and Online Safety Lead, the website/school blog/Seesaw Lead, IT technician, and Deputy DSL, will act as Online-Safety coordinators, although the overall responsibility is that of the DSL (Headteacher, Jill O'Connor).

Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

Definition of different technologies: websites, email, instant messaging, chat rooms, social media, mobile phones, apps, blogs, podcasts, downloads, virtual learning platforms.

The purpose and scope of the policy

This policy applies to all pupils, all teaching staff, all support staff, all governors and all volunteers.

Effective practice in online safety

Online safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils.
  All staff received online safety training with National Online Safety

- A comprehensive, agreed and implemented Online Safety Policy.

- Secure, filtered broadband via Coventry LA and a safe school network, overseen daily by our IT technician.

Aims

Our aims are to ensure that all pupils, including those with special educational needs:

- Will use the internet and other digital technologies to support, extend and enhance their learning;
- Will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- Will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- Will use existing, as well as up and coming, technologies safely.

Children with SEN have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. Class teachers will ensure that these children are well supported on a day-to-day basis, that they are taught in an appropriate manner to cater for their needs, about online dangers and keeping safe, and where issues arise around online safety, report immediately to DSLs. Incidents should also be logged on CPOMs. The SEN team, safeguarding team and learning mentors will help to support SEN pupils to ensure that they have a clear understanding about keeping safe and what they should do if they are worried.

Internet use will support, extend and enhance learning:

- Pupils will be given clear objectives for internet use.
- Web content will be subject to age-appropriate filters.
- Internet use will be embedded in the curriculum

Pupils will develop an understanding of the uses, importance and limitations of the internet:

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught how to report inappropriate web content.
- Online safety training will be embedded within the computing programme as part of the national Curriculum

Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working:

- Pupils will use the internet to enhance their learning experience.
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

Pupils will use existing technologies safely:

Pupils will be taught about online safety across the school, with supporting materials and resources from our 1Decision PSHE Program and our Rising Stars Online Safety Programme. Assemblies on online safety will also be delivered, as part of our

programme, teaching children about cyber-bullying, sharing personal data, appropriate communication/conduct and online grooming. This will be followed up in class with discussions and PSHE lessons.

Data Protection:

Please read our separate Data Protection policy.

Published content and the school web site:

The contact details on the Web site should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
The Headteacher, DSL and Website Lead, will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work:

Photographs that include pupils, will be selected carefully.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

***Email*:**

- Staff will only use approved email accounts, when using the school network.
- Pupils will only use email for approved activities.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Pupils will tell a member of staff if they receive inappropriate email communications.

Internet Access and Seesaw (VLP):

- Staff will read the online safety and acceptable usage policies along with relevant safeguarding policies and KCSIE 2021, before using any school ICT resource. Staff will sign to confirm these documents have been read.
- Parents will read and sign an internet access consent form, which includes acceptable usage expectations, before their children are given access to internet resources (including Seesaw).
- Pupils' internet access, during school hours will be supervised by a member of staff. Content published on Seesaw will need to be approved by members of staff.

Mobile Phones and other handheld technology:

Pupils are not permitted to have mobile phones or other personal handheld technology in school. Such items can be confiscated by school staff if they have reason to think that they are being used to compromise the wellbeing and safety of others (Education and Inspections Act 2006, Sections 90, 91 and 94).

Systems Security:

- ICT systems security will be regularly reviewed with support from the Local Authority, where necessary. Security strategies will be discussed with the Local Authority.
- Virus protection will be updated regularly.

Web Filtering:

The school will ensure that appropriate and robust filtering is in place.
Pupils will report any inappropriate content accessed to the Online Safety Lead and the Deputy DSL.

Communication of the online safety policy to pupils:

- Pupils will read (or have read to them) and sign the 'Acceptable Use' home-school agreement, before using these resources:

- Online-safety rules will be posted in each room, where a computer is used.
- Pupils will be informed that internet and Seesaw use will be monitored.

Communication of the online safety policy to staff:

- The online safety and acceptable usage policies will be given to all new members of staff as part of the staff induction handbook.
- The online safety and acceptable usage policy will be discussed with, and an agreement signed by, all staff.
- Staff will be informed that internet and Seesaw use will be monitored.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Communication of the online safety policy to parents/carers:

- The acceptable use policies will be available on the school website.
- Parents will be asked to read a home-school agreement when their children join the school. This will include expectations for acceptable usage relating to the internet, Seesaw and other digital technologies.
- The school will communicate and publicise online safety issues to parents through the school newsletters and website.

Online safety complaints:

Instances of pupil internet or Seesaw misuse should be reported to, and will be dealt with by, the Online Safety Lead, DSL or Headteacher.
Instances of staff internet (including inappropriate social media use) or Seesaw misuse should be reported to, and will be dealt with by the Headteacher.
Pupils and parents will be informed of the consequences of internet and/or Seesaw misuse.
Complaints of a child protection nature **must** be dealt with in accordance with school child protection procedures and reported **immediately** to the DSL or Deputy DSL.

Whole-School Responsibilities for Internet Safety:

Headteacher

- Responsible for online safety issues within the school but may delegate the day-to-day responsibility to other members of teaching staff – Online Safety Lead and Deputy DSL.
- Ensure that developments at Local Authority level are communicated to staff.
- Ensure that the Governing Body is informed of online safety issues and policies.
- Ensure that appropriate funding is allocated to support online safety activities throughout the school.

Governing Body

- Online safety will be reviewed as part of the regular review of child protection and health and safety policies.
- Support the headteacher, Deputy DSL or Online Safety Lead, in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
- Ensure that appropriate funding is authorised for online safety solutions, training and other activities, as recommended by the headteacher, Deputy DSL or Online Safety Lead, as part of the wider remit of the Governing Body with regards to school budgets).

Teaching and Support Staff

- Contribute to the development of online safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of online safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Embed online safety education in curriculum delivery.
- Know when and how to escalate online safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within & outside school.
- Take responsibility for their professional development in this area.

Wider School Community:

As a school we aim to encourage:

- This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet, Seesaw or other technologies.
- Contribute to the development of online safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.

- Develop an awareness of online safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Know when and how to escalate online safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Parents and Carers

As a school we aim to encourage:

- Contribute to the development of online safety policies, read online safety and safeguarding policies on the school website, and keep up-to-date with online safety information provided through the school website.
- Read acceptable use policies and encourage their children to adhere to them.
- Adhere to acceptable use policies when using the school internet and/or learning platform – Seesaw.
- Discuss online safety issues with their children, support the school in its online safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.
-

We ask parents to sign the agreement in appendix 1

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 senior leadership team should note that technologies such as mobile phones, with wireless Internet access, can bypass school filtering systems and present a new route to undesirable material and communications.

Children are not allowed to bring mobile phones to school, unless permission has been sought by parents for older children who need to walk home alone. In this instance, children will give their phones to their class teachers at the beginning of the school day to keep safe and this will be returned at 3.30pm. Children will be reminded that they **must not** use mobile phones on the school site.

Mobile phones will not be used during lessons or formal school time.

The sending of abusive or inappropriate text messages or files by Bluetooth/WhatsApp/Text Message or any other means is forbidden and will be followed up by a member of the Online Safety or Safeguarding team.

In school, iPads, iPods, Macs and Laptops are to be used to support teaching and learning. Programs such as FaceTime and messaging should not be used unless it forms part of a taught lesson.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Coventry LA can accept liability for any material accessed, or any consequences of Internet access.

Monitoring and review

The headteacher, deputy DSL, online safety leader and IT technician monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing board is responsible for approving this policy.

Appendix 1

Acceptable Use Policies

Part of the apparatus for Manor Park promoting online safety is a set of acceptable use policies (AUPs). These will be shared with pupils, parents, staff, governors, volunteers and visitors.

Acceptable use of the school's ICT facilities and internet: agreement for KS1 pupils and parents/carers	
When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Share my password with others or log in using someone else's name or password • Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I am following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Parent/carer agreement: By reading this agreement, you agree that your child can use the school's ICT systems and internet - when appropriately supervised by a member of school staff. You agree to the conditions outlined above, for pupils using the school's ICT systems and internet, and for using personal electronic devices in school. In addition, you will make sure your child understands these conditions.	

Acceptable use of the school's ICT facilities and internet: agreement for KS2 pupils and parents/carers

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Bully other people

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material, which might upset, distress or harm others or me.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Parent/carer agreement: By reading this agreement, you agree that your child can use the school's ICT systems and internet - when appropriately supervised by a member of school staff. You agree to the conditions outlined above, for pupils using the school's ICT systems and internet, and for using personal electronic devices in school. In addition, you will make sure your child understands these conditions.

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL), deputy DSL and online safety leader know if a pupil informs me they have found any material, which might upset, distress or harm them or others, and will do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

By reading this agreement, you confirm your understanding and acceptance of the above conditions.	

Acceptable use of the internet: agreement for parents and carers

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official website
- Our Twitter page
- Our virtual learning platform - Seesaw

Parents/carers also set up independent channels to help them stay on top of what is happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers 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

I will not:

- Use private groups, Seesaw, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, Seesaw, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

By reading this agreement, you confirm your understanding and acceptance of the above conditions.	