Manor Primary School

Online Safety

Policy and Audit

January 2023

IT / Computing Team

Based on documents from:
South West Grid for Learning
London Grid for Learning
Kent County Council

Introduction and Overview

Scope of the Policy

This policy applies to all members of our school community (including staff, pupils, volunteers, parents / carer, visitors, community users) who have access to and are users of school IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Our School Online Safety Policy

Our school's Online Safety policy will operate in conjunction with other policies including Behaviour, Bullying, Curriculum, Data Protection, Safeguarding, Information Security and any Home-School Agreements.

Effective Practice in Online Safety

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

- Education for responsible IT use by staff, pupils and families;
- A comprehensive, agreed and implemented Online Safety policy;
- A school network that complies with the National Education Network standards and specifications, with secure, filtered broadband;

Policy Review

- The Online Safety policy relates to other policies including those for IT, bullying, child protection and data protection.

- The Online Safety policy was last reviewed by: *Computing Team and Designated Safeguarding Lead.*

- It was approved by the Governors on: March 2023

- The next review date is (at least annually): *March 2024*

Online Safety Audit (2019-20)

Date of latest update of the Online Safety policy (at least annual): March 2023	
The school Online Safety policy was agreed by governors on: March 2023	
The policy is available for staff at: Staff Resources > Policies > Current up-to-date policies	
The policy is available for parents/carers at: School website	
The Online Safety coordinator is: William Davis and Kelly Baker	
The member of the Senior Leadership Team responsible for Online Safety is: William Davis	
The member of the Governing Body responsible for Online Safety is: Lili Khan	
The Child Protection are officers are: Nurun Khanom, Rohima Begum & Fiona James	
The Data Protection Officers are: Hardeep Hunjan	
Has Online Safety training been provided for all staff?	Y
Has Online Safety guidance been provided for all pupils?	Y
Are Online Safety guidance materials available for parents?	Y
Is there a clear procedure for a response to an incident of concern?	Y
Have Online Safety materials from CEOP and other agencies been considered?	Y
Have all staff (teaching and non-teaching) signed the Acceptable Use Policy?	Y
Have all pupils signed an Online Safety agreement form?	Y
Have all parents/carers signed an Online Safety home/school agreement form?	Y
Are Online Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y
Is Internet access provided by an approved educational Internet service provider (e.g. RM)?	Y
Has filtering on Internet-based devices been appropriately applied?	Y

Roles and Responsibilities

Headteacher:

- ✓ To take overall responsibility for Online Safety provision
- ✓ To take overall responsibility for data and data security
- ✓ To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements
- ✓ To be responsible for ensuring that staff receive suitable training to carry out their Online Safety roles and to train other colleagues, as relevant
- ✓ To be aware of procedures to be followed in the event of a serious Online Safety incident

Online Safety Coordinator / Designated Safeguarding Lead

- ✓ To take day to day responsibility for Online Safety issues and have a leading role in establishing and reviewing the school Online Safety policies / documents
- ✓ To promote an awareness and commitment to e-safeguarding throughout the school community
- ✓ To ensure that Online Safety education is embedded across the curriculum
- ✓ To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident
- ✓ Is regularly updated in Online Safety issues and legislation, and be aware of the potential for serious child protection issues
- ✓ To facilitate training and advice for all staff
- ✓ To liaise with the Local Authority and relevant agencies
- ✓ To communicate regularly with SLT and the designated Online Safety Governor

Governors / E-safety Governor

- ✓ To ensure that the school follows all current Online Safety advice to keep the children and staff safe
- ✓ To approve the Online Safety Policy and review the effectiveness of the policy
- ✓ To support the school in encouraging parents and the wider community to become engaged in Online Safety activities

IT / Computing Subject Leader

- ✓ To oversee the delivery of the Online Safety element of the Computing curriculum
- ✓ To liaise with the Child Safeguarding Lead

Network Manager / Technical staff / IT Subject Leader:

- ✓ To report any Online Safety related issues that arises, to the Online Safety coordinator
- ✓ To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy
- ✓ To ensure that provision exists for misuse detection and malicious attack, e.g. keeping virus protection up to date
- ✓ To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
- ✓ To check filtering lists are reviewed on a regular basis
- ✓ That the use of the network / internet / remote access / email to regularly monitored in order that any misuse / attempted misuse can be reported for investigation
- ✓ To keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant

Teaching and support staff

- ✓ To ensure they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- ✓ To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy
- ✓ To embed Online Safety issues in all aspects of the curriculum and other school activities
- ✓ To report any suspected misuse or problem to the Online Safety coordinator
- ✓ To ensure that any digital communications with pupils and parents / carers should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
- ✓ To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)
- ✓ To be aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- ✓ To maintain an awareness of current Online Safety issues and guidance e.g. through CPD
- ✓ To model safe, responsible and professional behaviours in their own use of technology

Pupils

- ✓ To read, understand, sign and adhere to the Pupil Acceptable Use Policy
- ✓ To understand the importance of reporting abuse, misuse or access to inappropriate materials, and how to do so
- ✓ To know, understand and adhere to the school policy on the use of mobile phones, digital cameras and hand held devices, including the taking of images and cyberbullying
- ✓ To understand the importance of adopting 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, if related to their membership of the school

Parents / Carers

- ✓ To support the school in promoting Online Safety and endorse the Parents' Acceptable Use Agreement, including the use of photographs and video images
- ✓ To consult with the school if they have any concerns about their children's use of technology

Community Users

- Any external individual / organisation will follow the Acceptable Use Policy when using any IT equipment or the internet within school

Policy Statements

Education – pupils

Our Online Safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and is provided in the following ways:

- ✓ A planned Online Safety curriculum is provided as part of Computing / PSHE / other lessons and should be regularly revisited
- ✓ Key Online Safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- ✓ Pupils sign and follow the guidance outlined in the Acceptable Use Policy

- ✓ Pupils are taught and encouraged to adopt safe and responsible use of technology both within and outside school, including appropriate online behaviour and keeping personal information private
- ✓ Pupils are taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- ✓ Staff act as good role models in their use of digital technologies, the internet and mobile devices
- ✓ In lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Education & training – staff & governors

Training will be offered as follows:

- ✓ Formal Online Safety training will be made available to staff during CPD sessions
- ✓ All new staff should receive a copy of Online Safety documents in their welcome pack. Ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements
- ✓ The Online Safety coordinator will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations
- ✓ This Online Safety policy will be presented to and discussed by staff in staff meetings
- ✓ The Online Safety coordinator will provide advice / guidance / training to individuals as required

Education – parents / carers

As a school we provide information and awareness to parents and carers through:

- ✓ Letters, newsletters, website, school APP
- ✓ Displays in school / at parents evenings
- ✓ Parent / carer Online Safety workshop / coffee morning
- ✓ High profile events such as Safer Internet Day
- ✓ Reference to the relevant websites / publications for further support

Managing the infrastructure

- ✓ The school network has user-defined policies ensuring secure documents are only accessible by specific users
- ✓ The school has educational, filtered, secure broadband connectivity
- ✓ Internet access is filtered for all users to keep users safe, including from terrorist and extremist material. Illegal content is filtered by the broadband provider, and nominated staff only are able to make a change to the filtering system
- ✓ The school will ensure, to the best of their ability, that the filtering system prevents pupils using websites designed to bypass the filtering
- ✓ The school has a secure wireless network to ensure access is restricted to school devices
- ✓ If staff or pupils come across unsuitable on-line materials, the site is reported to the appropriate person(s) in line with school policy
- ✓ The school checks their virus protection is updating regularly and informs their IT Support Service provider of any issues
- ✓ Staff and pupils have access to the school network via a login suitable to their 'role'. **Staff do not share their login details**
- ✓ Staff access to the management information system is controlled through a separate password for data security purposes. Staff only have access to the modules they require for their role, and passwords are not shared
- ✓ The school checks that their data is backed up

- ✓ The school is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- ✓ Pupils use a child-friendly internet search engine (e.g. kidrex)

Personal devices (including mobile phones and wearable technology)

- ✓ Personal devices brought into school are entirely at the owner's risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school
- ✓ Staff should not use their personal device when contacting pupils or parents; there should be access to a school phone
- ✓ The school strongly advises that pupils' mobile phones should not be brought into school
- ✓ The recording, taking and sharing of images, video and audio on any personal device is to be avoided, except where it has been explicitly agreed otherwise by the head teacher
- ✓ Personal devices **will not** be used when accompanied by children (including watches that contain built-in technology)

Use of digital and video images

- ✓ Parents / guardians sign the digital images agreement form to give their consent before photographs are used
- ✓ Digital media are used in accordance with the home school agreement
- ✓ The digital images agreement form is reviewed annually
- ✓ When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites
- ✓ Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- ✓ In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images
- ✓ Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Personal equipment of staff **will not** be used for such purposes
- ✓ Pupils must not take, use, share, publish or distribute images of others without their permission
- ✓ Photographs published on the website will be selected carefully and will comply with good practice guidance on the use of such images

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

- ✓ Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and any other relevant legislation

- ✓ The Headteacher is the Senior Information Risk Officer
- ✓ Staff must ensure that at all times they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- ✓ Staff must use personal data only on secure password protected computers and other devices, ensuring that they are properly ‘logged off’ at the end of any session
- ✓ Staff must ensure they only transfer data using encryption and secure password protected methods

Communications

- ✓ Staff should only use their school email account in communication with pupils and parents
- ✓ Staff or pupil personal contact information should not be published. The contact details given online should be the school office
- ✓ Staff should only use their school email account in any communication relating to school business
- ✓ Pupils should be taught about Online Safety issues such as the risks attached to the sharing or personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies

Social media – protecting professional identity

- ✓ The school has clear reporting guidance, including responsibilities, procedures and sanctions
- ✓ All school staff sign the acceptable use policy indicating they understand and will follow the guidance contained
- ✓ School staff ensure they make no reference in public social media to pupils, parents / carers or school staff
- ✓ School staff should not engage in online discussion on personal matters relating to members of the school community
- ✓ School staff should ensure that security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Social media – pupils

- ✓ The school will control access to social networking sites, and where relevant educate pupils in their safe use
- ✓ 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

Responding to incidents

- ✓ Complaints of internet misuse will be dealt with by a senior member of staff
- ✓ Any complaint about staff misuse must be referred to the head teacher
- ✓ Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- ✓ If a member of staff or pupil receives online communication that is considered particularly disturbing or illegal, the Police will be contacted
- ✓ Complaints related to cyberbullying will be dealt with in accordance with school bullying procedures
- ✓ Monitoring of incidents takes place and contributes to developments in policy and practice in Online Safety within the school

- ✓ Parents / carers are informed of Online Safety incidents involving children and young people for whom they are responsible

Appendix 1

E-safety in Computing programme of study

EYFS & Key Stage 1

Pupils should 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.

Key Stage 2

Pupils should be taught to:

- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- Use technology safely, respectfully and responsibly; recognise acceptable / unacceptable behaviour; identify a range of ways to report concerns about content or contact

For specific planning see:
Staff Resources > IT > Curriculum > Planning and Framework > Computing Framework