MANOR PRIMARY SCHOOL
Online Safety Policy

Manor Primary School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment. Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Manor Primary School we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Online Safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and computing environment for Manor Primary School.

Our Online Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

The Online Safety Policy and its implementation will be reviewed and approved by the Governing Body annually

It is to be used/read in conjunction with our other Safeguarding Policies:

- Acceptable use of Data & Computing Policy
- Anti-Bullying Policy
- Behaviour Policy
- Child Protection and Safeguarding Policy
- GDPR Policies
- Use of photographs and videos in school
- Social Networking Policy (ADOPTED WALSALL HUMAN RESOURCES – SCHOOLS)
- Code of Conduct (ADOPTED WALSALL HUMAN RESOURCES – SCHOOLS)

Roles and Responsibilities

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Head teacher and Senior Leaders:

- The Head teacher/SLT are responsible for ensuring the safety (including Online Safety) of members of the school community, though the day-to-day responsibility for Online Safety
- The Head teacher/SLT are responsible for ensuring that staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head teacher/SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head teacher/SLT should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made.
- The Head teacher/SLT liaise with school computing technical staff.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Head teacher for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be 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

Designated Safeguarding Lead:

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should 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

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to the E-Safety section of the website
- their children's personal devices in the school (where parental permission has been agreed)

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- All year groups are taught units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through computing we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through SLT & Governor meetings and also with individual teachers to ensure all children have equal access to succeeding in this subject. Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.

Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

- Pupils should be helped to understand that they need to adopt safe and responsible use both within and outside school.
- Staff should 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 should be 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education & Training

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:
A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.

- It is expected that some staff will identify online safety as a training need within the performance management process.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

Training – Governors

Governors should take part in online safety training / awareness sessions, This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school online training

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to Online Safety and agree to its use:

- All staff must read and sign the 'Acceptable computing User Agreement' before using any school computing resource.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the Head teacher, by recording the incident in an Online Safety Log, which will be stored in the Head teacher's office with other safeguarding materials. The Online Safety Log will be reviewed termly by the Online Safety Co-ordinator. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

Communication

When using communication technologies the school considers the following as good practice:

• The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others in school.

• Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

• Any digital communication between staff or parents / carers (email, social media, chat, blogs, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

• Pupils should be taught about online safety issues, such as the risks attached to the sharing of 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.

• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**

All users will be provided with a username and secure password.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place, for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems. These guest logins are managed by and are given out for temporary access and then removed at the end of the period of working in school.
  • An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Personal data should not be stored on removable devices e.g. children’s photographs, names and any reference to children.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff should be encouraged to change passwords regularly and can use a password manager as necessary to avoid password duplication.

Staff must always 'lock' the PC if they are going to leave it unattended.

Social Networking

Please see our separate Social Networking Policy

Reporting

All breaches of the Online Safety policy need to be recorded and reported to the appropriate staff member. The details of the user, date and incident should be reported. Incidents which may lead to child protection issues need to be passed on to the Head teacher immediately - it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require the Head teacher intervention (e.g. online bullying) should be reported to the Head teacher in the same day.

Allegations involving staff should be reported to the Head teacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline)

Handling Online Safety Complaints/Incidents

- Complaints of Internet misuse will be dealt with by the Head Teacher.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedure

Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse**. In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
  - Police involvement and/or action

• **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**

o incidents of 'grooming' behaviour
o the sending of obscene materials to a child
o adult material which potentially breaches the Obscene Publications Act
o criminally racist material
o promotion of terrorism or extremism o other criminal conduct, activity or materials
• **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Mobile Devices

Many new mobile devices can have access to the Internet. There are risks of mobile bullying, or inappropriate contact.

• Pupils by permission of the Head teacher can bring mobile devices onto the school site where it is seen by the school and parents as a safety/precautionary use. A school form is completed by the parent and the mobiles are handed into the school office at the start of the day and collected at the end of the day.

• The sending of abusive or inappropriate text messages is forbidden.

• Staff should always use the school phones to contact parents.

• All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day unless given express permission from Head Teacher.

• Staff may use their mobile phones in the staffroom during break/lunch time.

• Parents cannot use mobile phones in/around school - please see Use of photographs and videos in school policy

• On trips/offsite visits/swimming staff are provided with a school mobile that can be used for emergency only.

Digital/Video Cameras/Photographs

Please see our separate Use of photographs and videos in school policy and our Social Media Guidelines.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school website.
- Work will only be published with the permission of the pupil and parent. 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 (as such use in not covered by the Data Protection Act). 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.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

• School computing systems capacity and security will be reviewed regularly.

• Virus protection will be installed and updated regularly.

• Security strategies will be discussed with the Local Authority.

• Online Safety will be discussed with our computing support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the GDPR Policies.

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit computing use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

Communication of Policy

Pupils:

- Rules for Internet access will be posted in our ICT room.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during computing lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

All staff will be given the School Online Safety Policy and its importance explained.

Parents:

• Parents' attention will be drawn to the School Online Safety Policy in newsletters and on the school Website.

Link to behaviour policy

• The Education and Inspections Act 2006 empowers Head Teachers 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 cyber-bullying 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.

Policy Review

The policy was last reviewed and agreed by the Governing Body

November 2020 .