MANEY HILL PRIMARY SCHOOL

ONLINE SAFETY POLICY

Reviewed by Staff:	March 2023
Governor Ratification Date:	March 2023
Next Review Date:	March 2026

Our Vision

Maney Hill Primary School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. Maney Hill believes that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. Maney Hill aims to have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors and 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. We aim to establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Scope

This policy and related documents apply at all times to school equipment when accessing the internet and within the use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones. Online safety is viewed as a safeguarding issue and all members of staff have a duty of care to know the procedures and act upon these where appropriate.

Publicising online safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be either yearly or after policy updates
- Post relevant online safety information in all areas where technology is used
- Provide online safety information to parents / carers

Roles and Responsibilities

The Headteacher and the Governing Body have the ultimate responsibility for ensuring staff understand this policy and that it is being implemented consistently throughout the school. The role of computing leader has been delegated to Miss R Smithson and our Designated Safeguarding Leads are Mrs H Stonehill, Miss R Smithson, Miss J Green and Miss E Grencis. The Computing Leader and Safeguarding Leads are the

central point of contact for all online safety issues and act as the first point of contact for any online safety issues.

All members of school staff have core responsibilities within and outside the school environment. They should:

- Maintain an understanding of this policy and implement it consistently
- use technology responsibly; taking personal responsibility for professional development in this area
- have an awareness of a range of different online safety issues and how they may relate to the children in their care
- model good practice when using new and emerging technologies
- report any incidents to the Designated Safeguarding Leads using the school procedures
- understand that network activity and online communications are monitored, including any personal and private communications made via the school network
- be aware that staff have a duty to conduct themselves professionally and that misusing the internet may result in disciplinary action

The key responsibilities of children and young people are:

- respecting the feelings and rights of others both on and offline
- seeking help from a trusted adult if things go wrong, and supporting others who may be experiencing online safety issues at a level that is appropriate to their individual age, ability and vulnerabilities
- taking responsibility for keeping themselves and others safe online
- taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the Local Authority where appropriate.

- anti-virus software is installed on all computers and updated regularly
- central filtering is provided and managed by DNANet Support. All staff and students understand that if an inappropriate site is discovered it must be

reported to the DSLs who will report it to the DNANet Support to be blocked. All incidents will be recorded

- requests for changes to the filtering will be directed to the Headteacher, Assistant Headteachers or School Business Manager in the first instance who will forward these on to DNANet Support. Change requests will be recorded in the online safety log for audit purposes

- the school uses DNANet Support on all school owned equipment to ensure compliance with the Acceptable Use Policies

- all staff are issued with their own username and password for network access. Visitors / Supply staff are issued with temporary IDs and the details recorded in the school office

- Key Stage 1 pupils use class logon ID's for their network access
- Key Stage 2 pupils have their own username and password and understand that this must not be shared
- all pupils are issued with their own username/ password for Purple Mash software and other online resources such as TimesTable Rockstars

Educational Use

Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum approach to online safety.

In **Key Stage 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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of **primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The school's internet access is designed to enhance and extend education. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

- members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home

- pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

- the school will use age appropriate search tools

- the school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information

- the evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum

- the school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment

Mobile Phones, Laptops and iPads

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of staff at Maney Hill Primary School to take steps to ensure that mobile phones and personal devices are used responsibly.

- teaching staff at the school have access to a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times

- electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items

- to ensure the security of the school systems, personal equipment is not permitted to be connected to the school network

- new technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

- pupil iPads will have the app store disabled to ensure pupils have no ability to download new apps

- no social media should be downloaded onto staff or pupil iPads in any circumstance

- staff understand that they should use their own mobile phones sensibly and in line with school policy

- the sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the discipline/behaviour policy.

  ..\Behaviour policies\2022 Behaviour Policy.docx
  ..\Behaviour policies\2022 Anti-Bullying Policy.docx

- pupils' mobile phones will be permitted in school for safety reasons but they should not be used within the school grounds

- the sending of texts, messaging applications and any media files by pupils in school is not permitted

- pictures / videos of staff and pupils should not be taken on personal devices

- parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office

- pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers at the end of the school day.

E-mail

The school e-mail system is provided, filtered and monitored by Outlook 365

- all staff are given a school e-mail address and understand that this must be used for all professional communication

- pupils may only use school provided email accounts for educational purposes

- everyone in the school community understands that the e-mail system is monitored and should not be considered private communication

- staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the internet policy. In addition, they also understand that these messages will be scanned by the monitoring software

- everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher/ DSL as soon as possible

Published content

The Headteacher takes ultimate responsibility for content published to the school website. Class teachers and Key Stage Leaders are responsible for the editorial control of work published by their students.

- the school will hold the copyright for any material published on the school website or will obtain permission from the copyright holder prior to publishing with appropriate attribution
- the school encourages the use of e-mail to contact the school via the school office / generic e-mail addresses
- the school does not publish any contact details for the pupils

- written permission from parents or carers will always be obtained before images/videos of pupils are electronically published. We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.

Official videoconferencing and webcam use for educational purposes

The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

- all videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer

- videoconferencing contact details will not be posted publically

- video conferencing equipment will be kept securely and, if necessary, locked away when not in use

- school videoconferencing equipment will not be taken off school premises without permission

- staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure

Users

- pupils will ask permission from a teacher before making or answering a videoconference call or message

- videoconferencing will be supervised appropriately for the pupils' age and ability

- parents and carers consent will be obtained prior to children taking part in videoconferencing activities

- video conferencing will take place via official and approved communication channels following a robust risk assessment

- unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure

Content

- when recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely

- the school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class

Social Networking and Online Communication

Expectations regarding safe and responsible use of social media will apply to all members of Maney Hill Primary School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include social networking sites, blogs, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the school community

- all members of staff are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others

- any concerns regarding the online conduct of any member of staff on social media sites should be reported to the leadership team and will be managed in accordance with relevant policies

  ..\Management policies\2023 Teachers Code of Conduct.docx
  ..\Management policies\2023 Support Staff Code of Conduct.docx

- any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed.

Staff personal use of social media

- the safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities

- staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher

- any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead

- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites

- all members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential

- all members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school's policies and the wider professional and legal framework

- members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis

- members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school

- members of staff will ensure that they do not represent their personal views as that of the school on social media

- school email addresses will not be used for setting up personal social media accounts

Pupils use of social media

- personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes

- pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc

- pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present

- pupils will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications

- pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected

- the school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create any accounts within school or encourage their use

- any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour

- any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites

Engagement Approaches

Engagement and education of children and young people

- online safety teaching will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils

- education about safe and responsible use will precede internet access

- pupils input will be sought when writing and developing school online safety policies and practices

- pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability

- all users will be informed that network and Internet use will be monitored

- online safety will be included in the PSHE, SRE, Citizenship and Computing programmes of study, covering both safe school and home use

- safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas

- external support will be used to complement and support the school's internal online safety education approaches

Engagement and education of staff

- the online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities

- all members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or

institution into disrepute, or if something is felt to have undermined confidence in their professional abilities

- members of staff with a responsibility for managing filtering systems or monitor ICT use will have clear procedures for reporting issues or concerns

- the school/setting will highlight useful online tools which staff should use according to the age and ability of the pupils

Engagement and education of parents and carers

- Maney Hill Primary School recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology

- parents' attention will be drawn to the school online safety policy and expectations in newsletters, letters, school prospectus and on the school website

- a partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent online safety meetings and suggestions for safe home Internet use.

- Information and guidance for parents on online safety will be made available to parents in a variety of formats

- Parents will be encouraged to role model positive behaviour for their children online.

Responding to Online Incidents and Safeguarding Concerns

Emerging technologies offer a huge potential for teaching and learning opportunities but these should be appropriately evaluated to assess potential risks in addition to evaluating the educational benefits.

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Safeguarding Policy.

- all members of the community will be made aware of the range of online risks that are likely to be encountered including online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils

- all members of the school community will be informed about the procedure for reporting online safety concerns, such as breaches of filtering, cyberbullying, illegal content etc

- the Computing Leader and Designated Safeguarding Lead will be informed of any online safety incidents involving child protection concerns, which will then be recorded

- complaints about Internet misuse will be dealt with under the school's complaints procedure

- complaints about online/cyber bullying will be dealt with under the school's Behaviour and Ani-Bullying Policy

- any complaint about staff misuse will be referred to the headteacher

- all members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns

- all members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community

- the school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate

- the school will inform parents/carers of any incidents of concerns as and when required

- after any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required

- the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to West Midlands Police

- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated further

- parents and children will need to work in partnership with the school to resolve issues

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 2018

Full information regarding the schools approach to data protection and information governance can be found in the school's information security policy.

Wider Community

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and passwords that will be recorded in the School Office.