Mapplewell Primary School

E-Safety Policy

**Mapplewell Primary School Vision:**

"Developing a kind, respectful and happy community that promotes resilience and independence in all. Encouraging our pupils to leave Primary Education inspired and ready to contribute to the wider world."

|  |  |
| --- | --- |
| Date written | November 2022 |
| Date to be reviewed  | November 2023 |
| Date presented to Governors | *January 2023* |



**Introduction**

Mapplewell Primary School is committed to safeguarding all members of the school community. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Mapplewell Primary School educates children, parents and staff about the benefits, risks and responsibilities of using information technology

**How will Internet use enhance learning?**

Developing good practice in Internet use as a tool for teaching and learning is clearly essential. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils’ age and maturity. Often the quantity of information needs to be cut down and staff guide pupils to appropriate Web sites. Internet access is planned to enrich and extend learning activities. Pupils will be taught what Internet use is acceptable, how to use the internet safely and given clear objectives for Internet use. Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

**The role of the Headteacher:**

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e-safety Co-ordinator. The Headteacher(Designated Safeguarding Lead) and Deputy Safeguarding Lead are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. The Headteacher is responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant. The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. The Headteacher will receive regular monitoring updates from the E-Safety Co-ordinator.

**The role of the E-Safety Coordinator:**

The e-safety coordinator (Sam Garrood) takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. They ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place and provide training and advice for staff. When e-safety incidents are reported the e-safety coordinator creates a log to inform future e-safety developments.

**The role of the IT support team:**

The Trust IT support team is responsible for ensuring that the school’s technical infrastructure is secure and is not open to misuse or malicious attack. Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. They are responsible for ensuring that internet filtering is applied and updated on a regular basis and that the use of the network /internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of School for investigation.

**Teaching and Support Staff:**

Teaching and support staff are responsible for ensuring that they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices. That they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP). Staff must report any suspected misuse or problem to the Headteacher/E-Safety Coordinator for investigation, action or sanction. Any reported issues will be recorded and monitored on CPOMS by the Headteacher/E-safety Coordinator. All staff should ensure that safety issues are embedded in all aspects of the curriculum and other activities and that e-safety practises are modelled to pupils. Staff must ensure that pupils understand and follow the e-safety and acceptable use policies and that 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 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.

**Pupils:**

Pupils are educated in e-safety practises and responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy. They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Pupils 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. They should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-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 parent’s evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice.

**E-Safety**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school’s e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. The e-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

* A planned e-safety curriculum is provided as part of Computing / other lessons and is

regularly revisited

* Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
* Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
* Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged 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.

**Safeguarding our children on the Internet**

While the internet provides access to a world of new information and points of view, it also exposes young people to very real harms. Often children are left to access the internet without any supervision or controls and it can lead to danger from grooming, inadvertent exposure to graphic images, radicalisation and other online threats. So much time is now spent online that keeping children safe as well as enabling them to ‘stay children’ is paramount. The Safeguarding Policy for HCAT makes reference to such threats.

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf>

<http://www.proceduresonline.com/barnsley/scb/p_esafety_abuse_dig_media.html?zoom_highlight=internet>

**Technical – infrastructure / equipment, filtering and monitoring**

With guidance from the Trust IT support team 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 ensure that the relevant people named in the above sections will be effective in carrying out their e-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 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. Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. 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” (eg trainee

teachers, supply teachers, visitors) onto the school systems.

**Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement

policies to reduce the likelihood of the potential for harm. When using digital images, staff should 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. 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. 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. Pupils must not take, use, share, publish or distribute images of others without their permission. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Pupils’ full names will not be used anywhere on the school website, Mobile App or Twitter, particularly in association with photographs, unless express parental permission has been sought beforehand. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or on social media (covered as part of an agreement signed by parents or carers at the start of the year.)

**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 and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
* When staff send emails to outside agencies/contacts encryption must be used to protect email content and data. Staff must ensure that emails are sent to the correct person, if errors occur these must be reported immediately to the E-Safety Coordinator. Any attachments to emails must only be opened if the source is known and trusted.
* 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 and pupils or parents / carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems.
* Pupils should be taught about e-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.