BRADGATE
Education Partnership

Online Safety Policy

The Merton Primary School

Reviewed September 2025 by K.Johnson - Online Safety Lead

The Merton Primary School
To be the best we can be.

What we do

At The Merton Primary School, we encourage pupils and staff to use technology to support teaching and learning, including access to the internet. We also encourage and continue to explore ways of using technology to better streamline and improve our administration tasks. The online safety policy for The Merton Primary School is designed to help to ensure safe and appropriate access and usage for all Digital Technologies across the school community.

For the purpose of this policy, *Digital Technologies* are defined as electronic tools, systems, devices, platforms, and resources that generate, store, share, or process data. This includes, but is not limited to:

- Computers and laptops
- Tablets and mobile phones
- Cloud-based platforms and collaboration tools (e.g. Google Workspace, Microsoft 365)
- Email and messaging services
- Websites, blogs, forums, podcasts, and video-sharing sites
- Social media platforms
- Downloaded and streaming content
- Artificial Intelligence (AI) tools and virtual/augmented reality technologies
- Wearable devices and Internet of Things (IoT) connected technologies

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 online-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.

In addition, schools must operate in accordance with the UK GDPR and Data Protection Act 2018, ensuring that personal data held on digital devices is used and protected lawfully. Schools are also guided by Keeping Children Safe in Education (KCSIE), which sets out responsibilities for safeguarding pupils online, including managing filtering, monitoring, and reporting procedures.

Why do we have an Online Safety Policy?

With the ever increasing manner in the way technology is being used in education it is paramount that as educators we have in place policies and strategies which help us to keep both staff and pupils safe. We have highly functional school based and personal devices which give us access to powerful digital tools wherever we go. The internet and digital technologies provide valuable opportunities for learning, creativity, and connection due to its vast nature. However, they also present significant risks to children and young people if not used safely. Some of the dangers pupils may face include:

- Access to illegal, harmful or inappropriate content
- Access to content that promotes extremism and / or radicalisation
- Losing control over personal information, images or digital footprints
- The risk of grooming or exploitation by those with whom they make contact, exposing them to physical and sexual risk
- Exposure to, or engagement in cyber-bullying, harassment or online abuse
- Reliance on unreliable or misleading sources of information and a limited ability to evaluate the quality, accuracy or bias.
- Risks from newer technologies (e.g. AI, live streaming, gaming online scams or phising)
- Unhealthy online behaviours such as excessive screen time impacting health and wellbeing.

Other School Policies

This policy should be read in conjunction with other relevant school policies:

- Acceptable Use Agreement for adults - Guidance in Staff Reference Documents
- Acceptable Use Agreement for pupils – Displayed in classrooms
- Safeguarding policy
- Anti- Bullying policy
- PSHE policy
- Staff Code of Conduct
- GDPR policy

Legal Frameworks

It is the users' responsibility to ensure they are compliant and work within all UK and E.U. applicable legislation in regards to the safe and legal use of ICT in schools, this includes but is not limited to the following:

- The Sexual Offences Act 2003
- The Racial and Religious Hatred Act 2006
- The Computer Misuse Act 1990
- The Police and Justice Act 2006
- Communications Act 2003
- Malicious Communications Act 1988
- Copyright, Design and Patents Act 1988
- Public Order Act 1986
- Protection of Children Act 1978
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997.
- The Regulation of Investigatory Powers Act 2000 (RIPA)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education and Inspections Act 2006
- Equality Act 2010
- Education Act 2011
- Data Protection Act 2018
- UK GDPR
- Online Safety Act 2023
- Electronic Communications (Security Measures) Regulations 2022

Governor Responsibilities

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The schools Online Safety Governor will monitor compliance with this policy by:

- holding meetings with the Online Safety Co-ordinator / Officer
- attending Online Safety Group meetings
- monitoring of online safety incident logs
- monitoring of filtering / change control logs
- reporting to relevant meeting

School Leadership and Management Responsibilities

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer. The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. They are responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher / Senior Leaders 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. Primary World and Computing Lead to report any concerns to the Senior Leadership Team monthly or when concerns arise.

The Designated Safeguarding Lead (DSL) Responsibilities

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

Teaching and Support Staff Responsibilities

All trust staff shall make themselves aware of the content of this policy and attend relevant online safety training. Staff shall be responsible for contributing to the positive re-enforcement of e-safe behaviours through their day-to-day interaction with pupils and technology. Staff should act as good role models in their use of ICT, the Internet and mobile devices.

Where personal devices are allowed, all teaching staff shall ensure that pupils' use of these devices is for legitimate educational purposes and not for texting, accessing social networking sites or recording audio, video or still imagery without permission. Use of personal mobile phone is permitted to contact parents if necessary for example of school trips. This must be made as anonymous call by prefixing the number using 141.

All members of staff are provided with a school email address. Electronic communications with students, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Staff are advised to ensure that business correspondence is received to and sent from the school email address. This is to protect staff's privacy and ensure that school business is kept separate from private correspondence.

If staff are using approved AI tools for school purposes, they are aware of the importance of not sharing any confidential, personal or sensitive information.

As part of our safety culture, we complete and review a monitoring and filtering Risk Assessment Audit.

Parents and carers responsibilities

Parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/ regulation of their children's on-line experiences. Parents can often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the Internet and can be unsure about what they should do about it.

At The Merton Primary School we will therefore seek to provide information and awareness to parents and carers through:

- Relevant Online Safety links on the website
- Letters, newsletters, and other digital communications
- Parents evenings, Let's Connect Coffee Mornings / events
- Family learning courses in online safety, so that parents and children can together gain a better understanding of these issues.

System Management Responsibilities

The school, in conjunction with their ICT Support provider, will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that procedures set out within this policy are implemented: There will be regular reviews and audits of the safety and security of ICT systems. All users will have clearly defined access rights to the ICT systems of the school. This will be defined and accountable by the respective ICT lead /co-ordinator/s. Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to the schools Data Protection Officer.

The administrator passwords for the ICT system must also be available to the headteacher and kept in a secure, physical (e.g. fire safe) or electronic location software with encrypted storage. The School, in conjunction with the ICT Support provider, will use a sufficient internet filtering system to restrict access to certain materials, adhering to current government guidelines and recommendations. However, the school is aware that children must be educated in how to deal with inappropriate material.

Pupils Responsibilities

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 online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities. Online safety should be referenced in all areas of the curriculum and staff should reinforce online safety messages whenever ICT is being used:

A planned online safety programme will be provided as part of both Computing and PSHE lessons and will be regularly revisited – this will cover the use of ICT both in and outside school and will include:

- The safe and responsible use of the Internet,
- The safe and responsible use of mobile devices,
- The safe and responsible use of social media,
- The management of digital identity.

Whenever the Internet is used for research, pupils should be taught to be critically aware of the content they access on-line and be guided to validate the accuracy of information. It is accepted that pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request a temporary removal of those sites from the filtered list, for the period of study. Any request to do so should be auditable, time-limited and with clear reasons given.

Responding to incidents of abuse and misuse

At The Merton we understand the importance of acting on reported incidents of abuse and misuse of our ICT systems in school. These incidents may involve illegal or inappropriate activities. The school actively encourages a safe and secure approach to the management of incidents.

Pupils are encouraged to report any incidents immediately to a member of staff. Staff will liaise with senior management and the Designated Safeguarding Lead. ICT Support (where necessary) will investigate the alleged incident and establish evidence of any breach or wrongdoing. Staff will:

- Work with any pupils involved to resolve issues and educate users as necessary
- Inform parents/ carers of the incident and any outcomes
- Where the alleged incident involves staff misuse, the headteacher should be informed
- Outcomes of investigations will be reported to the headteacher and to external services where appropriate (e.g. Trust CEO, Social Services, Police Service, the Child Exploitation and Online Protection Service). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident

Useful Websites

Useful Websites:

www.gov.uk

In the search box type at the top of the page type:

- Preventing and tackling bullying
- Searching, screening and confiscation at school
- The Prevent Duty

www.leicestershire.gov.uk

In the search box at the top of the page type:

- E-Safety

www.thinkuknow.co.uk

Thinkuknow is the education programme from CEOP, a UK organisation which protects children both online and offline.

Explore one of the six Thinkuknow websites for advice about staying safe when you're on a phone, tablet or computer.

https://www.nspcc.org.uk/
In the search box at the top of the page type:

- Online Safety

https://www.internetmatters.org/

Acceptable Use Agreement for Governors and Volunteers

ICT and related technologies such as email, the internet and mobile devices are an expected part of working life in school. This agreement is designed to ensure that Governors and Volunteers are aware of their professional responsibilities when using any form of ICT.

Before becoming school ICT users, you are always asked to sign this policy and adhere to its contents. Any concerns or clarification should be discussed with the head teacher.

General:

I have read the school Online Safety Policy. I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will not install any hardware or software without the permission of online safety lead.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only take images of pupils and/or staff for professional purposes on school devices in line with school policy.
- I will not distribute images outside the school network/learning platform without the permission of the Head teacher.
- I will report any incidents of concern regarding children's safety to the Online Safety Lead, a Designated Safeguarding Lead or the Head Teacher.

Wi-Fi / Internet Use:

- I will only use the school's email / internet / intranet and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Head Teacher.
- I understand that I am responsible for all activity carried out under my username.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely including the use of AI technologies.
- I will not make copies or download any school-based information on my home devices.
- Personal or none data can only be taken out of school or accessed remotely when authorised by the Head Teacher or the Chair of Governing Body.

I agree to follow this code of conduct. I understand that the sanctions for disregarding any of the above will result in removal of access to ICT infrastructure and serious infringements may be referred to the police.

Full Name……………………………………………………………………………………………

……………………………………………… **Date**……………………………….................

Acceptable Use Agreement for Staff

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, carers and other professionals, they are asked to sign this agreement. Members of staff should consult the online safety policy for further clarification of their responsibilities.

- I understand that it is a criminal offence to use any school ICT resource for a purpose not permitted by its owner.
- I recognise that ICT includes school devices (iPads, laptops, cameras etc), cloud platforms, email, mobile phones, AI tools and personal devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the head teacher including taking home a class iPad.
- I understand that my use of school systems, internet and email may be lawfully monitored and recorded to ensure policy compliance.
- I will log off or lock devices when leaving them unattended.
- I will respect system security and not disclose any password or security information to anyone other than an authorised ICT support person.
- I will not install any software, apps or hardware without permission.
- I will store and share personal/sensitive data securely, only through school-approved systems whether in school, taken off site or accessed remotely.
- I will report any incidents of concern regarding children's safety online or using IT to a member of the Designated Safeguarding team or Online Safety Lead.
- I will not use personal email, messaging apps, or cloud storage for school business.
- I will use school email and platforms only in my professional role for communications with parents, and will not connect with pupils via personal social media or messaging.
- I will only use approved AI tools or emerging technologies and I will not share personal or sensitive data with AI systems.
- I will remain alert to cyber threats (e.g. phishing) and report suspicious activity to ICT support or the Online Safety lead.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude by modelling responsible ICT use.
- I understand that the school may monitor and review ICT use, including email and internet access, and may block or remove content if misuse or unlawful activity is suspected.

I agree to follow this code of conduct. I understand that the sanctions for disregarding any of the above will result in removal of access to ICT infrastructure and serious infringements may be referred to the police.

Full Name ………………………………………………….

Signature ………………………………………………….   Date…………………………….......

Acceptable Use Agreement for Pupils

At The Merton Primary School, we want you to enjoy using computers safely so it is important to follow these rules.

Our class promises to:

Always look after computers / computing equipment

Share computers /computing equipment fairly

Use kind language when talking to others online

CHOOSE kindness

Only use websites or play games with adult permission

Tell an adult if anything or anyone makes us feel uncomfortable or if there is a problem

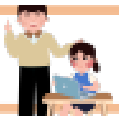
FAKE NEWS

Remember not everything we read online is true

Only click on icons and links that we know are safe

Only open attachments from people you know to avoid viruses or bugs

Only use the internet when an adult is nearby



***

Not share our usernames and passwords

Not bring to school any mobile phone or tablet from home unless it is handed into the office

Our Class Name:__________________________