Online Safety Policy

Mission Statement:

'In St Margaret Mary's School
we welcome everyone into our community
in order to live, love and learn
together in the light and example of the life of Christ.'

Policy to be reviewed July 2026

Our Vision

St. Margaret Mary RC Primary School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, St. Margaret Mary RC Primary School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises.

Related Documents:
Acceptable Use Policy
Behaviour Policy
Data Security Guidelines (BGFL guidelines)
Anti-bullying Policy
Birmingham City Council Internet Use Policy, Internet Use Code of Practice and Email Use Policy (linked from www.bgfl.org/esafety)

Policy Owner (DSL and Online Safety Co-ordinator): J.Logue & I.Travers
Implementation Date: September 2025
Review Date: July 2026

Aims
This policy document sets out the school's aims, principles and strategies for using the internet and protecting pupils.
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 communications with wider communities and business administration systems.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Staff and pupils have access to web sites worldwide offering educational resources, news and current events. There will be opportunities for discussion and exchange of information within the school community and others worldwide. Staff have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the Local Authority and Department for Education (DfE); receive up-to-date information and participate in government initiatives. The internet is also be used to enhance the school's management information and business administration systems.

Roles and Responsibilities
The Head and Governors have ultimate responsibility for establishing safe practice and managing Online Safety issues at our school. The role of DSLs/ Online safety coordinators has been allocated to J.Logue our designated senior person for child protection and members of the senior management team. They are the central point of contact for all Online Safety issues.

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

- Use technology responsibly.
- Accept responsibility for their use of technology.
- Model best practice when using technology.
- Report any incidents to the DSL/Online safety and Computing co-ordinator 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 in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

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 at least once a year or whenever it is updated
- Display relevant Online Safety information in each class through the SMART rules
- Provide Online Safety information in school and through the school website

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 LA where appropriate.

- Sophos anti-virus software is installed on all computers and updated regularly
- Central filtering is provided and managed by Link2ICT. All staff and pupils understand that if an inappropriate site is discovered it must be reported to the Computing co-ordinator who will report it to the Link2ICT Service Desk to be blocked.
- All incidents will be recorded in the Online Safety/Child protection log for audit purposes.
- Requests for changes to the filtering will be directed to the Computing co-ordinator in the first instance who will forward these on to Link2ICT or liaise with the Head as appropriate. Change requests will be recorded in the Online Safety log for audit purposes
- The School uses Policy Central Enterprise on all school owned equipment to ensure compliance with the Acceptable Use Policies.
- Pupils' use is monitored by the Computing Coordinator and Head Teacher
- Staff use is monitored by Computing Coordinator and Head Teacher
- All staff are issued with their own username for network access
- Visitors / Supply staff will be issued with temporary ID's
- All pupils are issued with their own username and password. They understand that this must not be shared.

Mobile / Emerging Technologies

- Teaching staff at the school are provided with a class laptop and iPad for educational use and their own professional development, which is kept in school. All staff understand that the Acceptable Use Policies (AUP) apply to this equipment at all times.
- Pictures / videos of staff and pupils must not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

E-mail

The school e-mail system is provided, filtered and monitored by Link2ICT is governed by Birmingham City Council E-mail Use Policy.

- All staff are given a school e-mail address (provided by BGFL365) and understand that this must be used for all professional communication
- 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 e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software. This also applies to the use of BGFL Teams.
- Pupils are assigned e-mail addresses to access Google Classroom, however the email facility has been disabled during set up.

Digital Media

- We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or videos are published or distributed outside the school.
- Photographs will be published in line with Becta guidance and not identify any individual pupil.
- Pupils' full names will not be published outside the school environment

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with 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.

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
• 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 in which they are using personal data.
• Sensitive personal pupil/staff data should never be taken off site without permission. In instances where permission is given, the personal data that is stored on portable computer systems, USB sticks or any other removable media should adhere to the following:
• The data must be encrypted and password protected

• The device must offer approved virus and malware checking software
• The data must be securely deleted from the device once it has been transferred or its use is complete

Educational Use

- School staff model appropriate use of school resources including the internet.
- All activities using the internet, including homework and the use of Google Classroom, independent research topics and other forms of online learning, will be tested first to minimise the risk of exposure to inappropriate material
- Where appropriate, links to specific web sites will be provided instead of open searching for information, pupils will be taught how to conduct safe searches of the internet
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Polices before any activity
- 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

The Use of the Internet to Enhance Learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- The school will control access to social media and social networking sites. Teachers are permitted to use twitter to share photos of pupils who have permission.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BCC can accept liability for the material accessed, or any consequences of Internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head teacher and Governors will ensure that the Internet policy is implemented and compliance with the policy monitored.

Pupil 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 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 education will be provided in the following ways:

- A planned online safety programme should be provided as part of Computing / PHSE / RSE /other lessons and should be regularly revisited – this will cover both the use of Computing and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies or lessons (Current use of Project evolve toolkit from Education in a Connected World 2020)
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils and parents will know about the Internet/acceptable use policy
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include: their real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils understand and follow the school Online safety and Acceptable Use Policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Pupils will be informed that Internet use will be monitored (Policy Central Enterprises) and that their use of Google Classroom for homework is also carefully monitored by teaching staff.
- Instruction in responsible and safe use should precede Internet access.

Staff Responsibilities

- All staff must accept the terms of the 'Birmingham Education Service Policy for Acceptable use of the internet'
- Staff will ensure they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP).
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by the Senior leadership team.
- All staff need have an up to date awareness of online safety matters and of the current school online safety policy and practices
- Staff must report any suspected misuse or problem to the Computing Co-ordinator/ DSL/ online safety coordinator or Head teacher for investigation / action / sanction
- Staff are 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
- In lessons where internet use is pre-planned and online learning, 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
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school's teacher handbook.

Responding to incidents

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

- Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour and Child Protection Policy.

- Any suspected illegal activity will be reported directly to the police. The Link2ICT Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head
- Breaches of this policy by staff will be investigated by the head teacher. Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by at least 2 senior members of staff.
- Pupil policy breaches relating to bullying, drugs misuse, abuse, prejudicial/discriminatory behaviour and suicide must be reported to the nominated child protection representative and action taken in line with school child protection policies. There may be occasions when the police must be involved.
- Serious breaches of this policy by pupils will be treated as any other serious breach of conduct in line with school Behaviour Policy. Referral to Heads of Phase may be appropriate at this level. Heads of Phase will also deal with email alerts generated by PCE (Policy Central Enterprises) for pupils. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- Minor Pupil offences, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy.
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate

I.Travers
This Online Safety Policy was devised and updated in September 2025
To be reviewed in July 2026