



Online Safety and Acceptable Use Policy

St Michael's Easthampstead CE Primary School

At St Michael's we are a community of active learners who go above and beyond in everything we do, equipping ourselves to make a difference in our own lives and in the lives of others

Policy Name	Online Safety and Acceptable Use Policy
Brief Description:	School's policies, procedures and responsibilities to promote online safety and the safe use of technology.
Status: Statutory/non-statutory	Statutory
Other related policies and procedures:	Safeguarding and Child Protection Behaviour Anti-Bullying Staff Code of Conduct Parent Code of Conduct Home School Agreement Data Protection policies Mobile Phone & Smart Technology Photography and Images permissions (inc. social media) Remote Learning
Approval level: HT/Governors/FGB	FGB
Approved by the Governing Board on:	14/7/2026
Frequency to be reviewed	Every 2 years
Latest Date for Next Review:	14/7/2028
Version + Schedule of Amendments:	4 – References to AI; emerging technology; mobile policy; UK GDPR and the Data Protection Act 2018
Signed:	Shaun Riordan
Position:	Headteacher
Date of Signature:	14/7/2026

Introduction

This Online Safety Policy relates to other policies including those for Computing, Anti- Bullying and Safeguarding and Child Protection. The Headteacher will oversee this area, with the Computing Subject Leader, and delegate where necessary. Our Online Safety Policy has been written by the school, building on government guidance. This policy also links to:

- Keeping Children Safe in Education 2025 (or current version when approved)
- Working Together to Safeguard Children
- Education Act
- Prevent Duty
- DfE Filtering and Monitoring Standards (2023 onwards)
- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018

Teaching and learning

• 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.

• Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Elements of our curriculum teaching include, but are not limited to:

- cyberbullying
- online grooming
- radicalisation
- misinformation
- fake news
- online scams
- Phishing
- Privacy settings
- gaming
- Livestreaming
- AI
- digital footprints
- healthy screen use
- consent
- sharing images
- online reputation

• The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

• Pupils will be taught what Internet use is acceptable and what is not. They will be given clear objectives for Internet use.

• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge

location, retrieval and evaluation

- Pupils will be taught how to evaluate Internet content
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully to minimize the risk that their image is misused. Staff will consider using group photographs rather than full-face photos of individual children. Pupil's faces may be blanked out, and it is recommended that photos are taken in side profile and/or back of the head.
- Pupils' full names will not be used anywhere on a school website or other non-secure on-line spaces, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or elsewhere.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils will be taught that social network sites have age restrictions, and Primary aged children should not have a profile on any social networking site.
- Pupils will be taught and advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when online.
- Pupils should not use mobile phones during the school day unless authorised by staff. Where pupils are permitted to bring phones to school, they must be handed to staff on arrival and collected at the end of the day in accordance with the school's Mobile Phone & Smart Technology Policy.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission from an adult.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled. • The forwarding of chain letters is not permitted.

Managing filtering

- The school works with our IT provider, TSI, to ensure systems to protect pupils are continuously reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher (as Designated Safeguarding Lead) or the Deputy Designated Safeguarding Lead.
- Senior staff and TSI will ensure that regular checks are made to ensure that the monitoring and filtering methods selected are appropriate, effective and reasonable.
- The school has appropriate filtering and monitoring systems in place that comply with the Department for Education Filtering and Monitoring Standards.
- Governors receive assurance that these systems are effective.
- The DSL, Headteacher and IT provider review filtering reports and incidents regularly.

Managing videoconferencing & webcam use

- Videoconferencing (including the use of Teams, Zoom and other approved video conferencing platforms) should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call or meeting invitation.
- Videoconferencing and webcam use will be supervised.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- The senior leadership team note that technologies such as mobile phones and smart watches with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Games machines including the PlayStation, Xbox, other internet-enabled gaming devices and others may have Internet access which may not include filtering. As a result, in line with our Mobile and Smart Technology Policy, these devices are not allowed in school by any pupil, staff member, parent, visitor or otherwise.

Artificial Intelligence

The school recognises that Artificial Intelligence (AI) tools are becoming increasingly common.

The school will ensure that:

- pupils are taught age-appropriate safe and responsible use of AI;
- staff understand both the educational benefits and safeguarding risks;
- AI does not replace professional judgement;
- confidential or personal information is never entered into public AI systems unless approved and compliant with UK GDPR and the Data Protection Act 2018;
- AI-generated material is checked carefully for accuracy and suitability;
- staff follow any additional guidance issued by the Headteacher regarding approved AI tools;
- AI-generated content should always be reviewed by a member of staff before being shared with pupils, parents or the wider community.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Authorising Internet access

- All staff must read and sign the “Acceptable Use Policy” before using any school IT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the school will be asked to sign an “acceptable use of school IT resources” before being allowed to access the internet from the school site.

Assessing risks and safeguarding

- The school will take all reasonable precautions to prevent access to inappropriate material, including the filtering and monitoring package implemented by TSI. 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 computer connected to the school network. Neither the school nor TSI can accept liability

for any material accessed, or any consequences of Internet access.

- The school will audit IT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.
- Online safety concerns will be treated as safeguarding concerns where appropriate and managed in accordance with the school's Child Protection and Safeguarding Policy.

Governance

Governors will:

- review this policy every two years
- receive regular safeguarding reports relating to online safety
- receive assurance regarding filtering and monitoring
- ensure statutory requirements are met
- support the school in promoting a culture of safe technology use.

Communications Policy

Introducing the Online Safety Policy to pupils

- Online rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Online training will be embedded within the Computing scheme of work as well as the Personal Social and Health Education (PSHE) curriculum.

Staff and the Online Safety Policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff who manage filtering systems or monitor IT use will be supervised by senior management and work to clear procedures for reporting issues. TSI reports will be sent to the Headteacher and / or SBM.
- Staff will promote the use of a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the updates in the school newsletters, and in any additional online safety newsletters.
- The school will maintain a list of Online resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents will be provided with online safety information and invited to attend workshops and awareness sessions whenever available.
- The school will support parents through:
 - newsletters
 - workshops
 - website resources
 - National Online Safety
 - UK Safer Internet Centre
 - Childnet
 - NSPCC guidance

Appendix 1

Pupil Guidelines for Internet Use

General

Pupils are responsible for good behaviour on the Internet, just as they are in the classroom or a school corridor. General school rules apply.

The Internet is provided for pupils to conduct research and communicate with others. Parents' permission is required. Remember that access is a privilege, not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards and will honour the agreements they have signed.

Computer storage areas and memory sticks will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or sticks will always be private.

During school, teachers will guide pupils towards appropriate materials. Outside school, families will bear responsibility for such guidance, as they must also exercise with information sources such as television, films, radio and other potentially offensive media.

The following are not permitted:

1. Sending or displaying offensive pictures or messages or pictures.
2. Using obscene language.
3. Harassing, insulting or attacking others.
4. Damaging computers, computer systems or computer networks.
5. Violating copyright laws.
6. Using others' passwords.
7. Trespassing in others' work folders, work or files.
8. Intentionally wasting limited resources.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on Internet use.
2. Additional disciplinary action may be added in line with the school's Behaviour Policy on inappropriate language or behaviour.
3. When applicable, the police or local authorities may be involved.

(Adapted from National Association for Co-ordinators and Teachers of Computing)

Go above and beyond with Love:
Kindness, Honesty, Respect and Aspiration

Appendix 2

Online Rules

- Ask permission before using the internet
- Tell a trusted adult if you see anything that makes you feel uncomfortable ▪ Immediately close any webpage that you are uncomfortable with
- Do not give out any personal information such as name, address, telephone number(s), age, school name or bank card details
- Make sure that when using social networking sites, privacy settings are checked so that not just anyone can see your page/photos
- Only contact people that you have actually met in the real world
- Never arrange to meet someone that you have only met on the internet
- Only use a webcam with people you know – Always ask an adult before using the camera function on a device
- Think very carefully about any pictures that you post online
- Never be mean or nasty to anyone on the internet or when using a mobile phone. If you know of someone being mean to another person, tell a trusted adult
- Only open e-mails from people that you know
- Avoid using websites that you wouldn't tell anyone about and use child-friendly search engines approved by the school.

Appendix 3

MANAGING INCIDENTS

The Online lead / DSL will ensure that an adult follows these procedures in the event of any misuse of the internet:

Has there been inappropriate contact?

1. Report to the designated Safeguarding Lead (or the Deputy)
2. Advise the child, young person or vulnerable adult on how to terminate the communication and save all evidence
3. Contact the parent(s)/carer(s)
4. Contact the police on 101
5. Log the incident on CPOMS
6. Identify support for the child, young person or vulnerable adult

Has someone been bullied?

1. Report to the designated Safeguarding Lead (or the Deputy)
2. Advise the child, young person or vulnerable adult not to respond to the message
3. Refer to relevant policies including anti-bullying, Online and AUP and apply appropriate sanctions
4. Secure and preserve any evidence
5. Contact the parent(s)/carer(s)
6. Consider informing the police on 101, depending on the severity or repetitious nature of the offence
7. Log the incident
8. Identify support for the child, young person or vulnerable adult

Cyberbullying

Cyberbullying is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages or e-mails either personally or anonymously, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e-mail. School will explain to pupils that this behavior is inappropriate and that, where appropriate, relevant people and professionals will be contacted (which may include the police and parents).

Has someone made malicious/threatening comments? (child/young person/vulnerable adult or organisation staff/volunteer)

1. Report to the DSL or Deputy
2. Secure and preserve any evidence
3. In the case of offending web-based e-mails being received, capture/copy the 'header' info, if possible.
4. Inform and request that the comments are removed from the site/block the sender
5. Inform the police on 101 as appropriate
6. Log the incident
7. Identify support for the child, young person or vulnerable adult

Has an inappropriate/illegal website been viewed?

1. Report to the DSL or Deputy
2. If illegal do not log off the computer but disconnect from the electricity supply to the monitor and contact the police on 101
3. Record the website address as well as the date and time of access
4. If inappropriate refer the child/young person/vulnerable adult to the AUP that was agreed and reinforce the message
5. Decide on the appropriate sanction
6. Inform the parent(s)/carer(s)
7. Contact the filtering software provider to notify them of the website (TSI)
8. Log the incident (CPOMS)
9. Identify support for the child, young person or vulnerable adult

Has an allegation been made against a member organisation staff/volunteer?

1. Refer to the Headteacher.
2. If the concern is about the Headteacher, refer to the Chair of Governors.

In the case of the above, the Bracknell Forest Safeguarding Board/ Safeguarding for Schools Procedures should be referred to (<https://bracknellforestsafeguarding.org.uk/>). All allegations should be reported to the organisation manager, police (101) and the Local Authority Designated Officer (LADO) (01344 352020), as appropriate.

Additional safeguarding actions

Where appropriate, contact:

- DSL
- LADO
- Police
- CEOP
- Children's Social Care

depending upon the nature of the concern.

Appendix 4

ACCEPTABLE USE POLICY (AUP) FOR STAFF AND VOLUNTEERS

Please sign and return to the School Office

This covers use of digital technologies in the organisation i.e., e-mail, internet, and network resources, learning platforms, software, mobile technologies, equipment and systems. Any questions you may have regarding Online or the acceptable use of the IT facilities in school should be directed to the Head Teacher / Designated Safeguarding Lead or to the Computing Subject Leader. TSI is the network manager. Where staff use personal devices for authorised school purposes (for example, but not limited to, 2FA purposes), they must comply with the school's Data Protection Policy, Staff Code of Conduct and this Online Safety Policy. Personal devices must not be used to store confidential pupil information unless expressly authorised.

By signing this form, you agree to the following conditions:

- I will only use the organisation's digital technology resources and systems for professional purposes or for uses deemed reasonable by the manager.
- I will only use an e-mail account allocated by the school, for school business.
- I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.
- I will report any accidental access, receipt of inappropriate materials or filtering breaches to the headteacher
- I will not allow unauthorised individuals to access e-mail / internet / networks of systems.
- I will ensure that all my login credentials (including passwords) are only shared with the IT Technician and Headteacher.
- I will not download any software or resources from the internet that can compromise the network or are not adequately licensed. I will speak to the IT Technician if I find software on the Internet I wish to have on my laptop.
- I will ensure that my personal e-mail accounts, mobile/home telephone numbers are not shared with children, young people or families.
- I will not allow children and young people to add me as a friend to their social networking site nor will I add them as friends to my social networking site.
- I will ensure that any private social networking sites / blogs, including Facebook and X (formerly Twitter) and other social media sites etc. that I create or actively contribute to are not confused with my professional role.
- I understand that all internet and network usage can be logged and this information could be made available to my manager on request. Ratified by Governing Body: February 2024 12 Review Date: February 2026
- I will not connect a computer, laptop or other device to the network/internet that has not been approved by the organisation and meets its minimum-security specification. Using your own USB is not permitted but, if agreement is authorized by the Headteacher/ School Business Manager to do so, I will ensure it is always scanned for viruses.
- I will not allow students to use a laptop / whiteboard that have been assigned to me. I understand that I will not loan my laptop to family members or friends.
- I will bring my laptop to work on a daily basis.
- If I no longer work at the school, I will return my laptop to the School Business Manager with all other electronic devices.
- Visitors to the school who require access to the internet can only do so with the permission of those named above.

- I will not use the IT facilities in school for personal reasons at any time when I am not on a timetabled break, including during directed time after school.
- I will not use personal digital cameras or camera phones for transferring images of children and young people or staff without permission from the Head. Any photos taken will be e-mailed to the Head (or a member of the SLT immediately) and then deleted from the individual device.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that the UK GDPR and the Data Protection Act 2018 requires that any information seen by me with regard to staff or children and young people, held within any organisation system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will at all times behave responsibly and professionally in the digital world and will not publish any work-related content on the internet.
- I will ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice.
- I understand that failure to comply with the Acceptable Use Policy (AUP) could lead to disciplinary action.

Social Networking Sites

- At home, I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role. I will not use these forums to make any comments in relation to the school, colleagues or students or to post any information relating to the school including photographs.
- I will only access social media for legitimate professional purposes authorised by the school, and must check with the Headteacher/ Designated Safeguarding Lead beforehand if I am unsure.
- I will not accept nor initiate 'Friend Requests' or 'Follows' from the parents of pupils or pupils themselves.
- I will not share information about the school in internet forums as it is unacceptable and can bring the school and / or the local authority into disrepute and put children at risk. If I see or become aware of inappropriate information about staff or children through conversations with colleagues, parents or partners, I understand that I have a responsibility to alert the school. I will keep this information confidential in line with the UK GDPR and the Data Protection Act 2018 and within the school's safeguarding policy. However, there may be times when I am required to disclose information to an appropriate authority such as the Police or Children's Social Care. In such cases, I can seek advice from the school's safeguarding officer or Local Authority HR

Staff must not

- use personal AI tools with confidential information
- use unapproved AI tools or software to process confidential school information
- photograph children on personal devices (except in authorised emergencies agreed in advance with the Headteacher and/or SLT)
- use WhatsApp or Messenger to communicate with parents
- use personal cloud storage
- use personal email for school information
- save school documents locally without encryption
- share passwords
- leave devices unlocked

Staff should

- lock screens when leaving devices
- report phishing emails
- complete annual online safety training
- use multi-factor authentication where available



Acceptable Use Policy

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Acceptable Use Policy (AUP).

I agree to abide by the school's most recent Acceptable Use Policy (AUP).

Signature Date

Full Name(print)

Job title

Organisation: St Michael's Easthampstead CE Primary School

Authorised Manager:

I approve this user to be set up

Signature: Date:

Full Name:

Job Title: (Headteacher/ School Business Manager)