Marshland Primary Academy

Online Safety Policy

1	Summary	Online Safety Policy			
2	Responsible person	Marta Speakman			
3	Accountable SLT member	Penny Marshall			
4	Applies to	☒All staff ☐Support staff ☐Teaching staff			
5	Who has overseen development of this policy	SLT			
6	Who has been consulted and recommended policy for approval	LGB			
7	Approved by and date	Autumn 2026			
8	Version number	4			
9	Available on	Every	☐Y ☒N	Trust website Academy website SharePoint	☐Y ☒N ☒Y ☐N ☒Y ☐N
10	Related documents (if applicable)	Safeguarding Policy			
11	Disseminated to	☒Trustees/governors ☒All staff ☐Support staff ☐Teaching staff			
12	Date of implementation (when shared)	September 2026			
13	Consulted with recognised trade unions	☐Y ☒N			

Contents

1. Introduction 4
2. Key Staff 4
3. Links to other policies and national guidance....4
4. Teaching and Learning 5
5. Staff Training....6
6. Support for Parents....7
7. Response to an online safety incident of concern....7
8. Email....7
9. Social Networking (Staff)....7
10. Publishing Pupils' Images and Work....8
11. Managing emerging technologies, mobile phones and devices....8
12. Managing ICT Systems and Access....9
13. Managing Filtering....9
14. General Data Protection Regulation (GDPR) and Online Safety....9

1. Introduction

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Marshland Primary Academy endeavours to highlight benefits and risks of using technology. We provide education and safeguarding of users to enable them to control their online experience.

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but in the wider world as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

Keeping Children Safe in Education (2026) identifies that the breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,

contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes,

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group

2. Key Staff

Marta Speakman – Computing Curriculum Lead

Penny Marshall – Principal and DSL

Jessica Taylor – Deputy Designated Safeguard Lead

Martin Oldknow – Safeguarding trustee

3. Links to other policies and national guidance

· Safeguarding and Child Protection Policy

· Whistleblowing Policy

· Behaviour Policy

· Staff Code of Conduct

· Venn GPDR Policy

The following guidance should also be read in conjunction with this policy:

· Keeping Children Safe in Education, September 2025

· Teaching Online Safety in School, January 2023

4. Teaching and Learning

Marshland Primary Academy uses a number of ways to teach and promote how to be safe online to all pupils:

· Online Safety unit in all year groups as outlined on the Computing Long-Term Plan, using

· Kapow (PSHE scheme)/ other lessons which have Online Safety related lessons embedded throughout

· Provide opportunities for regular open floor sessions in each class to discuss, remind or raise issues

· Celebrate and promote Online Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year

· Discuss, remind or raise relevant Online Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials

· Discuss, remind or raise with pupils information regarding use of social media, games and apps; and the dangers of taking part in online crazes

· Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas

· Pupils well be taught how to use a range of age-appropriate online tools in a safe and effective way

· Pupils, parents and staff reminded about their responsibilities through an Acceptable Use Policy which will sign and be displayed throughout the school

· All staff will model safe and responsible behaviour in their own use of technology during lessons

· Teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area

· When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content

· Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying

· Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

5. Staff Training

Our staff receive regular information and training on Online Safety issues, as well as updates as and when new issues arise

· As part of the induction process all staff receive information and guidance on the Online Safety Policy, the school's Acceptable Use Policy, online security and reporting procedures

· All staff will know what to do in the event of misuse of technology by any member of the school community

· All staff will be encouraged to incorporate Online Safety activities and awareness within their curriculum areas

All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of online safety. In particular:

· All staff should be aware of the indicators of abused/neglected including online

· All staff understands that online bullying can result in emotional abuse

· All staff know that sexual abuse can occur via the internet and involve a range of activities

· Staff should have an awareness of youth produced sexual imagery, known as sexting, and that this can be a sign of peer on peer abuse

· Staff should know how to respond to 'sexting' concerns appropriately

· Staff should be aware sexual harassment can take place online as well as off-line

· Staff should be aware the internet can play a role in gang activity

6. Support for Parents

Parents will be kept informed about online safety through advice in school newsletters, the school website and information workshops. The school website will be used to provide parents with useful information about keeping children safe online, with links to appropriate online safety websites and resources.

In the event of a concern being raised during online safety lessons or open floor sessions, these will be discussed with the parent by the class teacher and further information provided if required.

7. Response to an online safety incident of concern

An important element of online safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report online safety incidents so that they can be dealt with effectively and in a timely manner in order to minimise any impact.

The school has incident reporting procedures in place, including the secure electronic reporting system CPOMS. All staff have restricted access to the system but have the ability to report online safety issues at any time. Key members of staff have full access to the system, which allows the ability to respond, action and analyse incidents.

In the event of an online safety concern raised in school, parents will be informed and signposted to useful information. In the event of a serious online safety concern, the police will be informed in consultation with parents/carers. Concerns may also be raised with the UK Safer Internet Centre and CEOP.

8. Email

Staff will be allocated an email account for use in school. Staff will only use official school provided email addresses and should be aware that any use of the school email system can be monitored and checked. Staff should not use personal email accounts for professional purposes, especially to exchange any school related information or documents; or to email parents/carers. Staff should not send emails to pupils.

9. Social Networking (Staff)

Staff will not post inappropriate content or participate in any conversations which will be damaging to the school. They should not post, comment or share any material deemed to be offensive (sexual, religious, racist, homophobic etc). Doing so will

result in disciplinary action. Staff should not accept friend requests from pupils past or present.

The Marshland Instagram account is password protected and the password is shared with staff following approval from a member of the Senior Leadership Team. This is to give staff the ability to contribute to the school account.

10. Publishing Pupils' Images and Work

Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff. Staff will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs and videos. Written permission will be sought at the start of each year regarding the use of pupils' photographs on the school website and Instagram account.

Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.

11. Managing emerging technologies, mobile phones and devices

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

Staff

Mobile phones and other personal devices will not be used in any way during lessons or directed time. They should be switched off or on silent at all times. Smart watches should be disabled when teaching so the text and call notifications are off.

No images or videos will be taken on mobile phones or personally owned devices. Photographs and recordings can only be transferred from a school device and stored on a school computer/school network before printing.

The sending of abusive or inappropriate text, picture or video message is forbidden.

Pupils

Pupils should not bring mobile phones into school. If mobile phones are brought into school, the pupil will be required to hand them into the office at the start of the day and collected from the office at home time.

Pupils may be provided with school devices to use in specific learning activities under the supervision of a member of staff.

Parents/Carers

Parents are requested not use mobile phones or other personal devices when in school, where pupils are present.

In the case of school productions, parents/carers are permitted to take photographs of their own child in accordance with school protocols. These protocols strongly advise against the publication of any such photographs on social media sites.

12. Managing ICT Systems and Access

The school will agree on which users should and should not have internet access, and the appropriate level of access and supervision they should receive. All users will sign an Acceptable Use Policy, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour when using school ICT systems and that such activity will be monitored and checked.

Pupils may require usernames and passwords to access some online learning e.g. Reading Plus, TT Rock Stars etc. Usernames and passwords are provided to the pupils in the classroom. When these are shared for home use, this is done to a child's parents via an individual Parentmail message.

All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.

13. Managing Filtering

The school has a filtering system in place, which is managed by the school and Venn's ICT team. Banned phrases and websites are identified through this system and access blocked. The Principal receives daily Web Sweeper reports and is responsible for acting upon any breaches identified.

If staff or pupils identify an unsuitable website, it must be reported to the Online Safety Lead immediately. Any amendments to website access will be checked and assessed by the Online Safety Lead and members of SLT prior to being released.

14. General Data Protection Regulation (GDPR) and Online Safety

GPDR is relevant to online safety as it impacts on the way in which personal information should be stored on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to maintain the safety and security of personal data regarding all of the school population and external stakeholders. Personal and sensitive information should only be sent via email when on a secure network. Personal data should only be stored on secure devices.

All breaches of data must be reported to the Venn Data Protection Office (DPO) as soon as possible.