# Milverton Primary School

# Online Safety Policy 2023-2025

| | | |
|---|---|---|
| **Policy reviewed in** | **December 2023** | **Version #5** |
| **Policy due for review in** | **December 2024** | |

## Aims

Milverton Primary School wishes to allow children the opportunity to experience the vast enrichment that information technology can bring to their lives. This policy will outline how we are able to ensure this enrichment takes place under safe and responsible guidelines for staff, children and families to adopt, particularly in reference to KCSIE 2023.

The school views preparing children for safe and responsible use of information technology as a very high priority and maintains standards in line with the 360 safe accreditation.

Our Online Safety Policy has been written by the school, building on the current Warwickshire ICT Development Service Online Safety Policy and government guidance as well as guidance from KCSIE. It has been agreed by the school's senior management and approved by the governors.

Our Online Safety Policy will be reviewed annually – most recent review: July 2023.

Our approach to online safety is based on addressing the following categories of risk:

**Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.

**Contact** – being subjected to harmful online interaction with other users, such as 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as sharing explicit images and online bullying.

**Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Information and Communications Technology (Computing) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the school include (but is not limited to):

- Websites
- E-mail
- Image and video hosting and sharing websites
- Short-form video (YouTube Shorts, TikTok etc)
- Blogs and Wikis

- Podcasting
- Music streaming
- Gaming
- Mobile/ Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Given the range of internet-accessible devices, and platforms, children have access to both inside and outside of school, Milverton Primary School believes that encouraging children and young people to develop safe and responsible online behaviour from a very young age is ultimately the best defence for keeping them safe online.

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

Pupils will be taught about acceptable behaviour through both our computing curriculum, which includes both implicit and explicit learning opportunities about Online Safety, as well as being given clear objectives for Internet use, and sanctions for mis-use.

Children are taught about Online Safety on a termly basis as part of the computing curriculum but also taught discretely with small 'top-ups' within computing lessons. Our Online Safety curriculum is progressive throughout KS1 and KS2.

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.

Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. Children are also educated in this area, regarding Creative Commons licensing and similar. Full guidance can be found on:
http://www.copyrightandschools.org/

## Supporting Pupils with SEND and Vulnerable Pupils

As with our whole school curriculum, pupils with SEND or those having a more vulnerable profile are identified and supported as individuals, depending on their needs or circumstance. Where a member of staff is made aware of a pupil who requires alternative provision or support, this would be addressed through phase provision maps, and in conversation with school DSL's / SENDCO where relevant.

## Process for Dealing with Internet Misuse

Incidents where staff or children choose to access inappropriate material or break other terms of the ICT agreement or acceptable use policy, will be taken very seriously and dealt with in line with the school's behaviour policy, Online Safety Reporting Process, and staff discipline procedures. This may include incidents that take place outside of school but have an impact within the school community.

Reports of misuse inside or outside of school will be reported to parents and the school will support the family in re-educating children in safe practice. Internet misuse is also fed back to a DSL (the HT), and the governing body is made aware of these on a termly basis during HT updates at FGM meetings.

## Cyber Bullying

Where the school is made aware of cyber-bullying incidents, either in school or outside of school, this is manged comprehensively, through a meeting involving a DSL, pupils and parents. These incidents are also recorded on the Online Safety Issues log for reference if required. As a school, we encourage pupils or families to take screenshots of incidents themselves, to support conversations around resolution.

## Managing Internet Access

The security of the school information systems will be reviewed regularly by the Computing Lead and link governor, with relevant issues raised with a designated DSL, in this case the Headteacher. Background security services are reviewed and updated on an ongoing basis by the Local Authority. Virus protection is installed and updated regularly.

**Mobile Devices:** Children in year 5 and 6 who travel to school independently are allowed to bring a mobile device into school with them, which is handed into the school office at the start of each day and collected at the end. No mobile phone use is allowed by pupils between these times.

## Managing filtering

Internet traffic to Milverton comes via E2BN, who also provider KSCIE standard filtering, known as Protex. Detailed information regarding the level of filtering provided by Protex, and its adherence to KCSIE guidance, can be found at:

https://zammad.services.e2bn.org/help/en-gb/4-protex-web-filtering and

https://internet4schools.uk/wp-content/uploads/2021/06/2021-App-filtering-response.pdf

Protex also fulfils the logging elements of KCSIE monitoring guidance by providing access to reports based on the logged web traffic: https://zammad.services.e2bn.org/help/en-gb/11-protex-periodic-reports-how-to-get-access-to-reports

Such reports can be requested by school, if/when required.

## Monitoring

Monitoring products will complement Protex by giving more real-time feedback to school staff of individual activity across multiple media.

Regarding network monitoring using log files of internet traffic and web access - Protex fulfils this aspect of monitoring by providing access to reports based on the logged web traffic (as above). However, to improve the monitoring process, we have two additional features in beta at the moment (as of December 2023) that will do the following:

1. Send out once a day a summary/digest report to selected users of blocked activity
2. Near real-time alerts of blocked searches - checked at 5 minute intervals

If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the class teacher, and forward to the Head teacher.

## E-mail

Pupils may only use approved e-mail accounts, currently accessible through Microsoft 365, managed by our IT Support providers, 'Savvy IT'. These email accounts can be monitored by the class teacher if required.

Pupils must immediately tell a teacher if they receive an offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.

E-mails sent to an external organisation, whether written by staff or pupils, should be written carefully and, in the case of children, authorised before sending, in the same way as a letter written on school headed paper.

## Published Content and the School Website

All contact details on the school website, and on Weduc (school communication app) relate to the school. Staff or pupils' personal information will not be published.

The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name, other than on Weduc, where first names are used.

## Social Networking and Personal Publishing

Social networking sites and newsgroups will be blocked for children unless a specific use is approved by the Head teacher.

Pupils are advised (and taught explicitly in their Online Safety lessons) never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, social media accounts, e-mail address, names of friends, specific interests and clubs etc.

## Protecting personal data

Where applicable, personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Refer to the Data Protection policy for further information in this area.

## Authorising Internet access

All staff must read and sign the acceptable ICT use agreement, 'Online Safety Agreement Form for School Staff', on Weduc, before using any school ICT resource.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.

When a child moves into Year 3 children and parents will be asked to sign and return a form agreeing to follow the 'rules for responsible ICT use'.

## Assessing risks

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 breadth and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school will be guided by Warwickshire ICT Development Service to provide the best filtering and monitoring that is available to minimise risk in this area.

The Head Teacher will ensure that this Online Safety Policy is implemented and compliance with the policy monitored.

## Handling Online Safety complaints

Complaints of Internet misuse will be dealt with by a member of staff and recorded on the school's Online Safety Incident Log, which is also monitored by the governing body through the HT's termly report.

Any complaint about staff misuse must be referred to the Head Teacher.

Complaints relating to child protection must be dealt with in accordance with school child protection procedures, as outlined in the child protection policy.

## Introducing the Online Safety policy to pupils

Rules for Responsible ICT Use will be posted in the computer suite and shared with families upon entry to the school. Pupils will be informed that Internet use will be monitored.

Pupils sign to accept the school acceptable use guidelines from Y3 upwards. Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues. The integrity and safety of passwords will be explained and managed according to age and appropriate access. More information relating to passwords can be found in the passwords policy.

## Parents and Online Safety

As a school we recognise parental interaction plays a central role in children's behaviour online. We therefore recognise the importance of providing parents with up-to-date information to help families create a safe environment for children to explore the digital world at home. Ways in which this is achieved are through parent consultation meetings, and information sharing from wider agencies, such as the national 'Wake Up Wednesday' briefings.

## Staff and Online Safety

All staff have access to the School Online Safety Policy, and key messages through the acceptable use agreement. The importance of Online Safety is reinforced at appropriate intervals, and specifically for members of staff new to the school. The Online Safety policy specifies references to (and agreement with) the Password Policy, Video and Photograph Policy, and Staff/Governor Social Media Policy. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff members receive yearly Online Safety updates and briefings, shared through staff meetings and bulletin notes. The school's Online Safety Co-ordinator maintains up-to-date knowledge through attendance at professional development events, such as the yearly Warwickshire Online Safety conference.

This policy is the responsibility of the school's Online Safety Co-ordinator and reviewed by the Governing Body in rounds.