St Mary's Wavendon CofE Primary School

Online and Cyber Safety Policy

This is our school. With God's help we care for one another, are curious in our learning, and know we are all loved.

Luke 10:27 'Love the Lord your God with all your heart and with all your soul and with all your strength and with all your mind'; and, 'Love your neighbour as yourself.'

As a part of Inspiring Futures Through Learning Trust we adhered to all their policies and our school policies are adopted in conjunction with IFtL policies.

Policy name:		**SMW Online and Cyber Safety policy**
Version:		**V3**
Date relevant from:		**June 2025**
Date to be reviewed		**June 2026** **This policy will be reviewed every year unless legislation dictates otherwise. Recent changes in Legislation will need to be read and used to review this policy**
Role of reviewer:		**SMW Head of School & SMW Executive Head**
Statutory (Y/N)		**Y**
Published on website*		**Y**

Policy Level **:	**3**
Relevant to:	**All those within SMW school community**
Bodies consulted:	**School/ department governance bodies**
Approved by:	**SMW Governors**
Appr	

Key:

**** Publication on website:***

IFtL website		School website	
1	Statutory publication	A	Statutory publication
2	Good practice	B	Good practice
3	Not required	C	Not required

***** Policy level:***

1. Trust wide:
   - This one policy is relevant to everyone and consistently applied across all schools and Trust departments with no variations.
     - *Approved by the IFtL Board of Trustees.*
2. Trust core values:
   - This policy defines the values to be incorporated fully in all other policies on this subject across all schools and Trust departments. This policy should therefore from the basis of a localised school / department policy that in addition contains relevant information, procedures and / or processes contextualised to that school / department.
     - *Approved by the IFtL Board of Trustees as a Trust Core Values policy.*
     - *Approved by school / department governance bodies as a relevantly contextualised school / department policy.*
3. School / department policies
   - These are defined independently by schools / departments as appropriate
     - *Approved by school / department governance bodies.*

1. Aims

The first aid aims of our policy are to:

St Mary's Wavendon Primary School Online and Cyber Security Policy

Philosophy

Over the last few years, schools have become more and more reliant in IT systems and infrastructure to deliver critical services. At the same time, the threat from criminals and other bad actors has increased exponentially. As of May 2021, Microsoft monitoring of ransomware attacks revealed that 60% of all detected
attacks were aimed at schools and educational establishments.
This policy aims to set minimum standards for schools with the aim of ensuring that their systems are as protected as they can be against the threat of ransomware, malware and cyber−attack. Some of the language in this document may be technical but we have tried to keep it as understandable as possible.

At St Mary's Primary School the development of all children's social, moral, spiritual and cultural growth is paramount. We believe that the most important function of the school is to maintain an environment in which every member of the school is able to achieve success and self−fulfilment. There must be a total consistency of expectation that everyone (irrespective of gender, race or culture) should feel safe and secure, have empathy for all others, and place a high value upon individual achievement and personal development.

Safeguarding

At St Mary's Primary School, Child Protection and Safeguarding is paramount and we are fully committed to ensuring the welfare and safety of all our children. We believe that students have a right to learn in a supportive, caring and safe environment which includes the right to protection from all types of abuse, where staff are vigilant for signs of any student in distress and are confident about applying the processes to avert and alleviate any such problems. If any behaviour is a concern in relation to Safeguarding, St Mary's procedures and processes will be followed at all times in accordance with the Child Protection and Safeguarding Policy. Any concerns will be referred to the Designated Safeguarding Lead, Hannah King or the Deputy Designated Safeguarding Lead Claire McGonigle.

Our Safeguarding Governor is David Hopkins.

ICT Health, Safety and Welfare

The internet is becoming as commonplace as the telephone or TV in today's society; its effective use is an essential element in 21st Century life for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Our school has a duty to provide students with quality internet access as part of their learning experience.

Online safety includes, but is not limited to, browsing the internet. Other forms of electronic communication and interaction such as e−mail, blogging, social networking and online gaming should

be considered as well as the corruption, misuse, hacking and publication of personal data.

When using the internet, young people need to be protected from dangers including violence, racism and exploitation. Much of the material on the internet is published for an adult audience and therefore may be unsuitable for pupils. They need to learn to recognise and avoid any potential risks – to become "Internet Wise". Pupils need clear guidance in order to prepare them to respond appropriately to any situation, using any of the previously mentioned methods of electronic communication, for the inevitable moment when they come across inappropriate material or find themselves in an uncomfortable situation.

A clear school policy is required to help to ensure the safety of our staff and pupils. We have a requirement to provide pupils with as safe an environment as possible and a need to teach them to be aware of and how to respond responsibly to any of the risks.

- Writing, agreement and review of the E−Safety Policy

Our online Safety Policy has been written by the school using Local Authority and Government advice. It has been agreed by the SLT and Trustees. The policy and its implementation will be reviewed annually.

- Why the Internet and electronic communication use is important

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 functions. Internet use forms part of the statutory curriculum and as such is a necessary tool for learning.

The Internet forms part of everyday society and as such it is every schools' duty to prepare its pupils through quality Internet access with the personal tools to evaluate information and to take care.

There are benefits to the Internet and planned Government initiatives such as:

- Access to world−wide educational resources. (Museums or Galleries)
- Inclusion in the National Education Network connecting schools together
- The potential for world−wide educational materials and resources to enhance the National Curriculum
- Exchange of curriculum and assessment data between National Bodies
- Access school assessment, curriculum and personal resources from any location that has an internet connection
- The facility to extend learning beyond the traditional school building into an electronic environment

How the internet will be used to enhance learning:

- School Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils
- All Classes will be taught 'Rules for Responsible Internet Use', at the beginning of a school

year, and the skills needed in order to use the Internet appropriately. Internet access will be planned to enrich and extend learning activities, and pupils will be given clear objectives for all Internet use

- Pupils will be educated in the effective use of Internet in research, including the skills of knowledge location and retrieval
- Supervision is the key strategy, aimless surfing should never be allowed – pupils should always use the Internet in response to an articulated need
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the E−Safety Lead
- Schools should ensure that the use of the Internet derived materials by staff and pupils complies with copyright law
- Pupils will be taught to acknowledge the source of information and to respect copyright when using information from the Internet

The Online−Safety Lead and Service Provider will take reasonable steps to ensure

- Workstations will be configured to prevent user mistakes, deliberate actions or tampering Servers will be located in a locked room with only key personnel given access to the room.
- Virus protection systems will be provided, secured and kept up to date
- Access by wireless devices will be strictly controlled and ad−hoc access prevented through the use of authentication protocols
- The server operating system will be secure and kept up to date
- All inbound internet connections are configured to prevent unauthorised access
- Firewalls will be in place to prevent unauthorised access
- Files held on the school network will be regularly checked for content
- Monitoring of files and Internet usage will be handled in a professional and discrete way
- Breaches of protocols will be discussed and acted upon in collaboration with the E−Safety Lead and SLT
- The E−Safety Lead will review system security and capacity regularly
- Locally block access to websites or any other content that it deems inappropriate (the blocked list).
- Notify the company providing the internet filtering in the event of any inappropriate materials inadvertently being accessed via the Internet

Firewalls and Perimeter Protection

St Mary's Primary School has an appropriately configured firewall between our network and the internet . The router that is supplied by the broadband provider also contains the firewall.
All firewall and gateway devices have their default username and password changed to something appropriately secure (a hard to guess password with at least 8 characters) frequently. The new details are kept secure and only shared with those that need to know them (IT support staff or contractors).

Personal Data (to be read in conjunction with the IFtL General Data Protection Policy)

Personal data stored about staff, pupils and parents on the school network will only be accessed when needed for work purposes. Members of staff will only have access to this information in an appropriate way.
Only necessary staff, such as the ICT Technicians have access to BromCom's and other personal data that is held by the office.
Personal data can only be accessed via secure log−on and from a managed network. This ensures that sensitive information cannot be accessed when not linked to a school network.
"Zombie" accounts (accounts of staff who are no longer employed by the school,) are removed by the ICT Technician from when a member of staff is no longer an employee.

E−Mail

Directed e−mail use can bring significant educational benefits. However, the use of e−mail requires that appropriate safety measures are also put into place. All school provided e−mail accounts are filtered and subject to monitoring.

Pupils may only use approved e−mail accounts on the school system
Pupil access to external e−mail addresses is not permitted
Staff will be encouraged not to access external e−mail accounts at school. Any access during directed teaching time is strictly forbidden
Pupils must immediately tell a teacher if they receive an offensive e−mail
Pupils must not reveal details of themselves or others, such as their address or telephone number, or arrange to meet anyone through e−mail communication
Whole class or group e−mail addresses should be used when classes wish to contact external organisations or personnel
The forwarding of chain letters is banned
Official e−mail sent to parents should be written carefully and authorised before sending
Staff should ensure all emails sent to professional organisations are professional and courteous

The Management and Publication of Content

In this age, the use of websites to showcase a school and the work it produces has become extremely popular. However, it does provide opportunities acquiring sensitive and personal data if consideration is not given to the material available.

Unlike newspapers, the publication of pupil faces and full names is not acceptable. These published images could be re−used especially if a large image has been used. In addition to this, the publication of names and contact details of staff will be discouraged and where necessary, access to this information will be available via other methods or through a secure portal.

Only the schools contact details will be published. Staff or pupil contact information will not be published. The E−Safety Lead and SLT will take editorial responsibility and ensure content is accurate and appropriate. At all times, intellectual property and copyright rights will be respected and complied with.

- Under no circumstances is a pupil's full name to be published anywhere on a website, especially when it might relate to a photograph
- Parents will be given the right to 'opt out' of digital publication in any form of their child on the internet
- The 'opt out' information will be updated annually and records will be kept
- At all times, the pupil in photographs should, of course, be appropriately clothed

Social Networking and Personal Publishing

The recent upsurge in the popularity of social networking sites such as Facebook, Snapchat, Instagram and Twitter requires schools to be aware of the potential dangers to staff and pupils. It has become much easier for individuals to publish content and information about themselves on the Internet. The risk of identity theft and the misuse of published photographic material should be considered as risks by all and appropriate steps to educate and protect staff and pupils be made.

- All social networking sites will be blocked in school
- Consideration will be given, at all times, on how to educate pupils in their safe use
- Pupils will be advised never to give out information that will identify themselves, their friends or their location
- Pupils will be directed towards moderated sites
- Pupils will be advised to use nicknames and avatars when using social networking sites
- Pupils will be encouraged not to publish photographic content of themselves
- Staff should not identify pupils of their place of work in status updates
- Staff will be advised not to accept requests from current or past pupils
- Staff must not publish photographic content that contains any images from school or of pupils
- Staff should not publish status updates regarding school life

Filtering Internet Content

In a perfect world, filtering would be 100% accurate and inappropriate material would not be visible to pupils using the Internet. In practice, this is not easy to achieve and cannot be granted. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable and threatening. Such a procedure will be detailed further into the policy.

- The school will ensure systems are in place to filter website content
- The E−Safety Lead will make checks to ensure that the filtering is appropriate, effective and reasonable and this is monitored regularly
- A local school list will be maintained to further control the websites available within the school
- A local school list will be used to temporarily open access to websites for educational use by teaching staff. (all temporary access must be agreed with the technician and strict timings agreed)
- YouTube and other video content websites will be available in school for the use of teachers and support staff. Children are permitted to access YouTube or video content websites at school, but only with permission and supervision be a member of teaching staff

If for any reason, the filtering blocks a website that a class teacher feels would be of benefit to the children then it can be added to a whitelisted category and therefore be unblocked for teacher/pupil use. Such additions should be made to the E−Safety Lead who will make a decision on whether or not to add the website to the whitelist.

The school will also regularly monitor the websites that children access. By producing a monthly list of the most visited websites a picture of the usage and activities of the children can be obtained. The list of websites will be reviewed monthly and when appropriate, additional domains and websites may be added to the blocked list.

Videoconferencing and Webcams

The rapid expansion of communications technology requires the school to have a policy on its potential use in education.

- All videoconferencing and webcams must make use of the school network to ensure quality of service and security.
- Teachers must request permission from SLT before making a call or using a webcam in a lesson.
- All webcam use will be supervised.
- At no point will any live streaming from school be permitted to be viewed on the Internet or through the school website

Managing new technologies

Small wireless devices provide more opportunities for pupil to be exposed to content within school that cannot be controlled or filtered through the school network or security systems. This can even extend to games consoles used in after school care clubs where it is possible to connect to global gaming networks and interact with other people. At all times we need to be aware of the current technology and its possible risk and educational benefit.

- Pupils' mobile phones will be stored in a locked tin or cupboard throughout the day
- The use of cameras in mobile phones is not permitted
- A blog may only be used in school by pupils if it is appropriately moderated
- The school will ensure its network will block connections from devices that are not part of its domain. (Personal laptops, iPads, iPod touches, wireless mobiles)
- The use of 3G broadband devices is not permitted as it will bypass all school filtering systems

The Prevent Duty and Online Safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the wellbeing of any pupil is being compromised.

Protection of Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act (DPA) 1998 and the General Data Protection Regulation (GDPR) 2018.

Authorisation of Internet Access

Staff need to be vigilant and ensure that any use of the Internet by pupils must be authorised and supervised at all times. This will ensure that any potential risks are reduced and that a pupil will have

an immediate point of contact should they have a problem or are uncertain of action to take. All staff and pupils must be made aware of the rules and regulations surrounding the use of any ICT resource before beginning to use it in education.

- All staff will ensure that they have read and signed a 'Staff Code of Conduct for ICT'
- All pupils will be taught about internet safety and will sign a 'class agreement'
- At all times a record of staff and pupils who are granted access to the school network will be maintained
- Any person not employed by the school must be made aware of the rules and acceptable use of ICT systems before being allowed access

Risk Management

At all times staff, pupils and parents should be made aware that:

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

Regular audits of ICT use will establish if the e−safety policy is adequate and that the implementation of the policy is appropriate and effective.

Online Safety complaints

- Staff misuse will be referred to the Head of School
- Complaints made about Internet misuse will be dealt with by the E−Safety Lead and SLT
- Complaints of a child protection nature must be dealt with in line with the school Child Protection Procedures
- Parents and pupils will be informed of any necessary complaints procedure
- Parents, pupils and staff will be made aware of the consequences of the misuse of the Internet or school resources

Regulation

The use of a limited and expensive resource, which brings with it the possibility of misuse, must be regulated. Fair rules, prominently displayed will help pupils to make responsible decisions

- Rules of Internet access and E−mail use will be posted near all computer systems
- Pupils will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede all Internet and E−mail access
- Staff will be made aware of their responsibilities through the distribution of the online safety policy
- Staff will be informed that Internet use can be monitored
- Monitoring will be carried out by the E−Safety Lead working to clear procedures for reporting issues
- Parents/carers will be made aware of the School's online safety policies

Abuse of the System

Any transgressions of the rules which are minor can be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and sanctions available include:

- An interview/counselling by a member of SLT
- Informing parents or carers
- The removal of Internet or computer access for a set period of time

Approval: Online and Cyber Policy 2025 This policy was ratified by the Governors Date: 10th June 2025 Signed: HAYLEY COOK & DAVID HOPKINS	Next Review on or before: September 2026 *This policy will be reviewed annually and approved by the Governors at on an annual basis.*