Online Safety Policy

White Spire School

Written by:	M.Bartle
Last reviewed on:	Sept 2025
Next review due by:	Sept 2026

Contents

1. **KEY CONTACTS in school/setting**

Name	**Role**	**Contact details**
Headteacher	Michelle Bartle	01908 373266
Chair of governing body	Shanie Jamieson	01908 373266
Designated safeguarding lead (DSL)	Anton De Beer	01908 373266
Out of hours contact for DSL	Safeguarding Team	safeguarding@whitespire.milton-keynes.sch.uk
Deputy DSL	Michelle Bartle	01908 373266
Other members of the safeguarding team (DSLs')	Sophie Lunnon Sally Elton Karen Richards Laura Halsey Katie Marlborough	01908 373266
Prevent lead	Anton De Beer	01908 373266
Child sexual exploitation lead	Anton De Beer	01908 373266
Child Looked After/ Previously Looked After	Anton De Beer	01908 373266
Mental health lead	Anton De Beer	01908 373266
Designated governor for safeguarding	Tanya Stevens	01908 373266
Designated governor for mental health and well being	Tanya Stevens	01908 373266
Safer recruitment governor	Shanie Jamieson	01908 373266
ICT Curriculum Lead	Rebecca Fensom	01908 373266
IT Support	IT Support	itsupport@whitespire.milton-keynes.sch.uk

2.Introduction

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2025–(KCSIE) and other statutory documents; it is designed to sit alongside the school's Child Protection Policy.

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

This policy applies to all members of White Spire School (including staff, volunteers, contractors, pupils, parents/carers and visitors) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

3. Aims

This policy aims to:

- Set out expectations for all White Spire School Members of online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
- For the protection and benefit of the children and young people in their care.

4. Roles and Responsibility

All members of White Spire School have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour.

Headteacher

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead
- Ensure that policies and procedures are followed by all staff
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DSL and senior management team, ICT Systems support to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented

- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure that there is a system in place to monitor and support staff (e.g. DSL team) who carry out internal technical online-safety procedures
- Ensure the school website meets statutory requirements.
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHCE/ Relationships and Sex Education curriculum, complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHCE and Relationships and Sex Education.

DSL

- "Liaise with the local authority and work with other agencies in line with Working Together to Safeguard Children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the head teacher and senior management team, ICT Systems support to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged on C-POMS
- Ensure the 2021 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and Annex A
    - Online Safety Training

All Staff

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are

- Ensure that key safeguarding responsibilities are following which includes reading and implements KCSIE (Part 1, Annex A all staff and full document DSL's, Head teacher and Governors)
- Complete key Online Safety training
- Read and follow this policy in conjunction with the school's main Child protection policy
- Record online safety incidents in the same way as any safeguarding incident (C-POMS)
- Sign and follow the staff code of conduct
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities
- Whenever overseeing the use of technology (devices, the internet) encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL/OSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online safety issues (particularly relating to bullying and sexual harassment and violence) in the playground corridors and other areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

ICT Curriculum Lead

As listed in the 'all staff' section, plus:

- Oversee the delivery of the online safety element of the Computing curriculum
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach

ICT Systems Support

As listed in the 'all staff' section, plus:

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / ICT curriculum Lead to ensure that school systems and networks reflect school policy

- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the head teacher
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Report an online safeguarding concerns/ blocked activity to a DSL.

5. Online safety

It is essential that at White Spire School children and vulnerable young adults are safeguarded from potentially harmful and inappropriate online material. At White Spire School, we have a whole school approach to online safety that protects and educates pupils, students, and staff in their use of technology and have a range of ways to identify, intervene in, and escalate any concerns (follow schools Child Protection Policy).

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

• Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, hate speech, radicalisation and extremism.

• Contact: being subjected to harmful online interaction with other users; 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: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

• 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 (https://apwg.org). (KCSIC 2025)

Furthermore there is disinformation which is the deliberate creation and spread of false or misleading content, such as fake news. Misinformation is the unintentional spread of this false or misleading content. It is important that we teach our pupils that not all information online in fact.

6. Handling Online Concerns

It is vital that all staff recognise that online-safety is a part of safeguarding. Concerns must be handled in the same way as any other safeguarding concern and staff must follow the schools safeguarding procedures...

White Spire School's procedures for dealing with online-safety are mostly detailed in the following policies (primarily in the first key document):

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy
- Sexual Violence and Harassment Policy
- Child Sexual Exploitation/Child Criminal Exploitation Policy
- E-Security

White Spire School commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's procedures.

Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day.

Any concern/allegation about staff misuse is always referred directly to the Head teacher, unless the concern is about the Head teacher in which case the complaint is referred the LADO (Local Authority's Designated Officer)/Chair of Governors. Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police). We will inform parents/carers of online-safety incidents involving their children in line with the schools Child Protection Policy.

7. Behaviour

Bullying of another person will be treated with the highest severity. Please refer to the schools Anti-Bullying and Sexual Violence and Harassment Policy.

8. Teaching and Learning

The following subjects have the clearest online safety links:

- PSHCE
- Relationships and Sex Education
- Computing

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.
- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Any student blocked activity is directly reported to the ICT Systems Manager via Securely. Staffing blocked activity is monitored via Opendium Web Gateway. This will then be report to a member of SLT. The schools filtering system prevents pupils from accessing blocked activity.
- Pupils will be taught what Internet use is acceptable and what is not and 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 shown how to publish and present information to a wider audience.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content by reporting to a member of staff or parent who will take the necessary action.
- It is the role of all staff to identify opportunities to thread online safety through all school activities making the most of learning opportunities.
- Whenever overseeing the use of technology all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers.

At White Spire School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum. Annual reviews of curriculum plans / schemes of work are used as an opportunity to focus on the key areas.

9. Managing Internet Access/Equipment

Monitoring

- The school reserves the right to monitor the use of the network, internet and e-mail systems. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being breached, appropriate action will be taken.

Property

- Pupils and staff should treat any property belonging to the school with respect and reasonable care and report any faults or breakages to the ICT Systems Manager.

Viruses

- Pupils and staff should be aware of the potential damage that can be caused by computer viruses. Pupils and staff must not download, install or run any programs or data (including computer games) or open emails from unknown or unidentifiable sources.

Leaving workstations

- If a person leaves their workstation for any period of time they should lock their workstation.

Information system security

- School ICT systems security is reviewed regularly by the ICT Systems Manager.
- Virus protection is automatically checked by the provider, Sophos. This is checked daily and updated when necessary.
- Security strategies will be discussed with the Local Authority when requested.
- All computers and laptops are password protected.
- Pupils should not attempt to gain unauthorised access to anyone else's user area or to any information which they are not authorised to access.

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. Children have use of their Google accounts which can be accessed via ICT systems manager.
- All incoming e-mail should be treated as suspicious. Attachments should not opened unless the author is known and the attachment is expected. The same applies to embedded links in emails. If anyone is unsure about the contents of an email, they should contact the ICT Systems Manager.
- Pupils are taught how e-mails from and to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

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

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other online space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- School keeps a list of pupils whose image are not permitted to be used for any purpose including Internet publications.

Social networking and personal publishing

- The school controls access to social networking sites, and educates pupils in their safe use at home through the teaching of Online Safety in ICT lessons.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils currently do not use social networking sites in school.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for special needs pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites at home.
- Staff must not use social networking sites in school.

Managing filtering

- Web filtering & DNS is managed through Opendium's Web Gateway product and Securly on Chromebooks.
- Google "Safe Search" (a Google feature) is enforced to prevent inappropriate content being found.
- E-mail services are provided by Google who perform rigorous checking of incoming/outgoing email.
- If staff or pupils come across unsuitable online materials, the site must be reported to the ICT Systems Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- Pupils use Google Meet (part of Google Workspaces for Education), ensuring quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

Managing emerging technologies/AI

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by an appropriate member of the ICT Team before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Personal mobile phones will not be used during lessons or formal school time (Reception-Y11), the sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones is not permitted.

- Games Consoles, for example in After School Club, are not connected to the Internet as their use may not include filtering.
- Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils. All staff have access to cameras to take photographs.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to General Data Protection Regulation 2018.

10. Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the global 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 Milton Keynes Council can accept liability for any material accessed, or any consequences of Internet access.

- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

11. Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

12. Community use of the Internet

- If the need arises the school will liaise with local organisations to establish a common approach to Online Safety.

13.Communications

Introducing the Online Safety policy to pupils

- Online safety 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.
- A programme of training in online safety is in place and is based on the materials from CEOP.
- Online safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHCE) curriculum.

Staff and the Online Safety policy

It is vitally important that staff are careful about content that they search out or download. Staff need to ensure that films or other material shown to children are age-appropriate. Staff must be aware of their responsibilities to the school when using social networking sites such as Facebook. Our staff code of conduct and confidentiality policy must be adhered to at all times, even outside of working hours. Disciplinary action could result if the school is brought into disrepute.

- Staff must not post anything on any online site that could be construed to have an adverse impact on the school's reputation.
- Staff must not post photos related to the school on any internet site including pupils, parents, staff or the school branding (uniform).
- Staff must not form online friendships with pupils and parents.
- Staff must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school.
- Staff will be required to complete Online Safety training.
- Staff should use their school email account for all school-related communications. Email is provided for school related purposes only.
- Staff to be aware of the various members of staff responsible for Safeguarding issues.
- Staff members should refer to the Staff Code of Conduct for more detailed information.
- All staff are given the School Online Safety Policy and its importance explained.
- Staff are informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be managed by senior management and work to clear procedures for reporting issues.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School Online Safety Policy in the school brochure and on the school Web site.
- The school will maintain a list of Online Safety resources for parents/carers. See appendix 2.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

14. Policies

The Online Safety policy should be read in conjunction with a range of specific policies (but not limited to)

- Child Protection Policy
- Relationship and Sex Education Policy
- PSHCE Policy
- E-Security Policy
- PREVENT Policy
- Staff Code of Conduct

Appendix 1: Quick Guide to Online Safety in School

Activities	Key Online Safety issues	Relevant websites
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Google (enforced safe search)
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. School filtering systems provide online moderation.	School Provided Account Kent Learning Zone
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on "moderated sites" and by the school administrator.	Headline History Kent Grid for Learning National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Learning grids Museum sites, etc. Digital Storytelling BBC – Primary Art National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	Google Meet for Education
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	National Archives "On-Line" Approved Google Hangouts Vidyo Lifesize

Appendix 2: Useful resources

BBC Stay Safe

www.bbc.com/ownit

General Internet safety site

www.childnet.com

Child Exploitation and Online Protection Centre

www.ceop.gov.uk

Digizen – responsible digital citizen

www.digizen.org

Think U Know

www.thinkuknow.co.uk

Safer Children in the Digital World

www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Appendix 3: Useful resources for parents

Care for the family

www.fosi.org

Internet Watch Foundation

www.iwf.org.uk