



Online Safety Policy

Date reviewed: February 2024

Next review date: February 2026

Contents

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Educating pupils about online safety
5. Educating parents/carers about online safety
6. Cyber-bullying
7. Acceptable use of the internet in school
8. Pupils using mobile devices in school
9. Staff using work devices outside school
10. How the school will respond to issues of misuse
11. Training
12. Monitoring arrangements
13. Links with other policies

Appendix 1: online safety training needs – self-audit for staff

Appendix 2: online safety incident report log

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others

- › Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- › Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- › [Teaching online safety in schools](#)
- › [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- › [Relationships and sex education](#)
- › [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study. At St Wystan's School, we use Purple Mash to cover the programmes of study. Online safety also forms part of our PSHCEE curriculum which is planned using the guidelines from the PSHE Association.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with the SLT and Blue Box what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet. Acceptable user agreements can be found at this the following link ([ICT and internet acceptable user policy.doc](#) see Appendices 2-5)

- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

At St Wystan's School, the DSL is the Headteacher and the DDSL is the Deputy Headteacher. Details of the school's designated safeguarding leads (DSL/DSSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with Blue Box to make sure the appropriate systems and processes are in place
- Working with the Blue Box, and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see Appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

- Updating and delivering staff training on online safety contains a self-audit for staff on online safety training needs (see Appendix 1)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the SLT and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 Blue Box

Blue Box, as the School's service provider, is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks. Ensuring these are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check, and monitoring the school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Advising the School on the most effective and up-to-date methods of filtering and monitoring. The alteration of the filtering and monitoring system is at the School's discretion.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use. The acceptable user agreements can be found at this the following link [ICT and internet acceptable user policy.docx](#)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting directly to the DSL.
- Following the correct procedures by contacting the Operations Manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately, in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- › Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet. The IT and acceptable use policy can be accessed at the following link: [ICT and internet acceptable user policy.doc](#) (see appendices 2-5)

- › Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
- › What are the issues? – [UK Safer Internet Centre](#)
- › Hot topics – [Childnet](#)
- › Parent resource sheet – [Childnet](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet connection will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable user. The IT and acceptable use policy can be accessed at the following link: [ICT and internet acceptable user policy.doc](#) (see appendices 2-5)

4. Educating pupils about online safety

In Pre-Prep, pupils will be taught to:

- › Use technology safely and respectfully, keeping personal information private
- › Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In Prep, pupils will be taught to:

- › Use technology safely, respectfully and responsibly
- › Recognise acceptable and unacceptable behaviour
- › Identify a range of ways to report concerns about content and contact

By the end of Form 6 pupils will know:

- › That people sometimes behave differently online, including by pretending to be someone they are not
- › That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- › The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- › How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- › How information and data is shared and used online
- › What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- › How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

The online safety curriculum, as taught at St Wystan's, is outlined below:

	PSHCE	Purple Mash
Rec	<ul style="list-style-type: none"> • keeping passwords safe 	
Form 1	<ul style="list-style-type: none"> • how and why people use the internet • the benefits of using the internet and digital devices • how people find things out and communicate safely with others online 	Prior and Future Learning Links - Unit 6.2 - Online Safety.pdf
Form 2	<ul style="list-style-type: none"> • the ways in which people can access the internet e.g. phones, tablets, computers • to recognise the purpose and value of the internet in everyday life • to recognise that some content on the internet is factual and some is for entertainment e.g. news, games, videos • that information online might not always be true 	Prior and Future Learning Links - Unit 6.2 - Online Safety.pdf
Form 3	<ul style="list-style-type: none"> • how the internet can be used positively for leisure, for school and for work • to recognise that images and information online can be altered or adapted and the reasons for why this happens • strategies to recognise whether something they see online is true or accurate • to evaluate whether a game is suitable to play or a website is appropriate for their age-group • to make safe, reliable choices from search results • how to report something seen or experienced online that concerns them e.g. images or content that worry them, unkind or inappropriate communication 	Prior and Future Learning Links - Unit 6.2 - Online Safety.pdf
Form 4	<ul style="list-style-type: none"> • that everything shared online has a digital footprint • that organisations can use personal information to encourage people to buy things • to recognise what online adverts look like • to compare content shared for factual purposes and for advertising • why people might choose to buy or not buy something online e.g. from seeing an advert • that search results are ordered based on the popularity of the website and that this can affect what information people access 	Prior and Future Learning Links - Unit 6.2 - Online Safety.pdf
Form 5	<ul style="list-style-type: none"> • to identify different types of media and their different purposes e.g. to entertain, inform, persuade or advertise • basic strategies to assess whether content online (e.g. research, news, reviews, blogs) is based on fact, opinion, or is biased • that some media and online content promote stereotypes • how to assess which search results are more reliable than others • to recognise unsafe or suspicious content online • how devices store and share information 	Prior and Future Learning Links - Unit 6.2 - Online Safety.pdf

Form 6	<ul style="list-style-type: none"> • about the benefits of safe internet use e.g. learning, connecting and communicating • how and why images online might be manipulated, altered, or faked • how to recognise when images might have been altered • why people choose to communicate through social media and some of the risks and challenges of doing so • that social media sites have age restrictions and regulations for use • the reasons why some media and online content is not appropriate for children • how online content can be designed to manipulate people's emotions and encourage them to read or share things • about sharing things online, including rules and laws relating to this • how to recognise what is appropriate to share online • how to report inappropriate online content or contact 	Prior and Future Learning Links - Unit 6.2 - Online Safety.pdf
--------	--	--

At St Wystan's we also have a legal obligation to teach:

- [Relationships education and health education](#) in primary schools

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety via Parent Hub and other communications home, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' meetings and workshops.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher or Deputy Headteacher.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. [9a Behaviour Policy.docx](#)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers and staff teaching computing will discuss cyber-bullying with their form.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information, via Parent Hub, on cyber-bullying to parents and carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from Headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Headteacher, to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy / searches and confiscation policy – [9a Behaviour Policy.docx](#)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

St Wystan's School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

St Wystan's will treat any use of AI to bully pupils in line with our anti-bullying policy. [10a Anti-bullying Policy.docx](#)

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Pupils using mobile devices in school

Pupils are not permitted to bring mobile phones or smart devices into school. Any such devices seen in school will be confiscated and returned only to the parent or carer. The only exception would be if a pupil travels alone and a mobile device is required for safety reasons. In this situation, the mobile device will be stored in a locked space by the class teacher throughout the school day, from their arrival on the premises, and only given to the pupil as they leave school for the day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

8. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:

- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

➤ Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

9. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 2

This policy will be reviewed every 2 years by the Headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

10. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy [7a Safeguarding Policy .docx](#)
- Behaviour policy [9a Behaviour Policy.docx](#)
- Staff disciplinary procedures – [Staff Discipline, Conduct and Grievance Policy .docx](#)
- Data protection policy and privacy notices [GDPR and Data Protection Policy.docx](#)
- Complaints procedure - [33a Complaints procedure.docx](#)
- IT and internet acceptable use policy – [ICT and internet acceptable user policy.doc](#)

Appendix 1: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	

ONLINE SAFETY TRAINING NEEDS AUDIT

Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 2: online safety incident report log

ONLINE SAFETY INCIDENT LOG

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident