St Wystan's
A REPTON SCHOOL

E-SAFETY ONLINE POLICY

This policy includes the Early Years Foundation Stage (EYFS) and After School Care (ASC)

Policy Reviewed: January 2021 (Updated August 2021)

Policy to be reviewed: January 2023

1 **Aims**

The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which:

- protects the whole School community from illegal, inappropriate and harmful content or contact;
- educates the whole School community about their access to and use of technology; and
- establishes effective mechanisms to identify, intervene and escalate incidents where appropriate.

2 **Scope and application**

This policy applies to the whole School including the Early Years Foundation Stage (**EYFS**).

This policy applies to all members of the School community, including staff and volunteers, pupils, parents and visitors, who have access to the School's technology whether on or off School premises, or otherwise use technology in a way which affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

This policy relates to current and emerging technologies and includes, but is not limited to, websites, email, instant messaging, blogging, social networking sites, chat rooms, media downloads, gaming sites, text and picture messaging, video calls, podcasting, online communities, mobile devices, cloud technologies and online learning platforms.

3 **Regulatory Framework**

This policy has been prepared to meet the School's responsibilities under:

- Education (Independent School Standards) Regulations 2014;
- Statutory framework for the Early Years Foundation Stage (DfE, September 2021);
- Education and Skills Act 2008;
- Childcare Act 2006;
- Data Protection Act 2018 and General Data Protection Regulation (GDPR); and
- Equality Act 2010.

This policy has regard to the following guidance and advice:

- Keeping children safe in education (DfE, September 2021);
- Preventing and tackling bullying (DfE, July 2017);
- Sexting in schools and colleges: responding to incidents and safeguarding young people (UK Council for Child Internet Safety, August 2016);
- Prevent duty guidance for England and Wales (Home Office, July 2015);
- Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, April 2015).
- Sexual violence and sexual harassment between children in schools and colleges (DfE, December 2017); and
- Searching, screening and confiscation: advice for schools (DfE, January 2018).

The following School policies, procedures and resource materials are relevant to this policy:

- Acceptable use of ICT policy for pupils;
- Acceptable use of IT policy for staff and staff guidance on using social media;
- Safeguarding and child protection policy;
- Anti-bullying policy;
- Risk assessment policy for pupil welfare;
- Staff code of conduct and whistleblowing policy;
- Data protection (GDPR) policy for staff.
-

4 **Publication and availability**

This policy is published on the School website and is available in hard copy on request. A copy of the policy is available for inspection from the school office during the School day. This policy can also be made available in large print or another accessible format if required.

5 **Definitions**

Where the following words or phrases are used in this policy:

References to **Designated Safeguarding Lead** are references to the Designated Safeguarding Lead for School. In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as **technology**). See above for examples of the types of technologies covered by this policy.

6 **Responsibility statement and allocation of tasks**

The Board of Governors has overall responsibility for all matters which are the subject of this policy.

They are required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Governors response to this duty.

To ensure the efficient discharge of its responsibilities under this policy, the Board of Governors has allocated the following tasks:

Task	**Allocated to**	**When / frequency of review**
Keeping the policy up to date and compliant with the law and best practice	IT Coordinator	As required, and at least termly
Monitoring the implementation of the policy, including the record of incidents involving the use of technology and the logs of internet activity and sites visited	Bluebox/ IT Coordinator	As required, and at least termly
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the GDPR	Operations Manager	As required, and at least termly
Seeking input from interested groups (such as pupils, staff, Parents) to consider improvements to the School's processes under the policy	IT Coordinator	As required, and at least annually
Formal annual review	Head/ Board of Governors	Annually

7 **Role of staff and parents**

Head and Senior Leadership Team

The Head has overall executive responsibility for the safety and welfare of members of the School community.

The Designated Safeguarding Lead is the senior member of staff from the School's leadership team with lead responsibility for safeguarding and child protection, including online safety. The responsibility of the Designated Safeguarding Lead includes managing safeguarding incidents involving the use of technology in the same way as other safeguarding matters, in accordance with the School's safeguarding and child protection policy.

The Designated Safeguarding Lead will work with the IT Coordinator (see below) in monitoring technology uses and practices across the School and assessing whether any improvements can be made to ensure the online safety and well-being of pupils.

The Designated Safeguarding Lead will periodically collect information from staff, pupils and parents to inform updates to the policy and online safety procedures.

The Designated Safeguarding Lead will regularly monitor the technology incident log maintained by the IT Coordinator, provided by Lightspeed.

The Designated Safeguarding Lead will regularly update other members of the School's Senior Management Team on the operation of the School's safeguarding arrangements, including online safety practices.

IT Coordinator

The IT Coordinator is responsible for ensuring that:

(a) the user may only use the School's technology if they are properly authenticated and authorised;

(b) the School abides by the regulations set out in; https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

(c) the risks of pupils and staff circumventing the safeguards put in place by the School are minimised;

(d) the use of the School's technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation;

(e) The IT coordinator will report regularly to the Senior Leadership Team on the operation of the School's technology. If the IT coordinator has concerns about the functionality, effectiveness, suitability or use of technology within the School, including of the monitoring and filtering systems in place, they will escalate those concerns promptly to the Designated Safeguarding Lead.

(f) The IT coordinator is responsible for maintaining the technology incident log (a central record of all serious incidents involving the use of technology) and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's safeguarding and child protection policy.

IT Support

Bluebox IT is responsible for ensuring that:

(a) Office 365 will provide a security overview in terms of email usage and the type of email traffic that is sent and received by the school. This includes information around areas such as malware content.

(b) they provide automated monitoring of the school server and networks. Any critical issues will be alerted to our remote support team who will review and action accordingly under the school's support agreement.

(c) The IT Coordinator receives a weekly email from the web filtering software listing users who have visited inappropriate sites or tried to download inappropriate content. The IT coordinator will escalate concerns to the DSL.

(d) the School's technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack;

Bluebox are responsible for the effective operation of the School's filtering system so that pupils and staff are unable to access any material that poses a safeguarding risk, including terrorist and extremist material, while using the School's network.

All staff

All staff have a responsibility to act as good role models in their use of technology and to share their knowledge of the School's policies and of safe practice with the pupils.

Staff are expected to adhere, so far as applicable, to each of the policies referenced in this policy.

Staff are responsible for promoting and supporting safe behaviours in their classrooms. When pupils use school IT or technology whilst in the care of school, staff should ensure that supervision is appropriate for the pupils involved.

Staff should raise concerns about online safety with the IT coordinator or Designated Safeguarding Lead.

Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's safeguarding and child protection policy.

Parents

The role of parents in ensuring that pupils understand how to stay safe when using technology is crucial. An IT agreement is sent out to parents and children. The School expects parents to promote safe practice when using technology and to:

(a) support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;

(b) talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour; and

(c) encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

If parents have any concerns or require any information about online safety, they should contact the Designated Safeguarding Lead. They can also consult the online safety resources detailed in section 11.

8 **Access to the School's technology**

The School provides internet and access to Purple Mash and Spelling Shed to pupils and staff, and an email system to staff as well as other technology. Pupils and staff must comply with the respective acceptable use of IT policy when using School technology. All such use is monitored by the IT coordinator and Head.

Pupils and staff require individual user names and passwords to access the School's network and internet, Purple Mash accounts and email system which must not be disclosed to any other person. Any pupil or member of staff who has a problem with their user names or passwords must report it to the IT coordinator immediately.

The Ubiquiti Managed Wi-Fi system w.ill log information on all devices connected to the school's main secure network or Guest network. This can be queried by device type and MAC address details, time of access and amount of information downloaded via the wi-fi network.

The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which may change, must be obtained from a member of staff in order to use the Wi-Fi.

Use of mobile electronic devices

The School has appropriate filtering and monitoring systems in place to protect pupils using the internet (including email and social media sites) when connected to the School's network.

Mobile devices equipped with a mobile data subscription can provide unlimited and unrestricted access to the internet. Since the School cannot put adequate protection for pupils in place, St Wystan's School pupils are not permitted to have mobile phones in School under any circumstances;

The School rules about the use of mobile electronic devices are set out in the acceptable use of ICT policy for pupils.

The use of mobile electronic devices by staff is covered in the code of conduct.

The School's policies apply to the use of technology by staff and pupils whether on or off School premises and appropriate action will be taken where such use affects the welfare of other pupils or any member of the School community or where the culture or reputation of the School is put at risk.

9 **Procedures for dealing with incidents of misuse**

Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

Misuse by pupils

Anyone who has any concern about the misuse of technology by pupils should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the anti-bullying policy where there is an allegation of cyberbullying.

Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's safeguarding and child protection policy).

Misuse by staff

Anyone who has any concern about the misuse of technology by staff should report it in accordance with the School's whistleblowing policy so that it can be dealt with in accordance with the staff disciplinary procedures.

If anyone has a safeguarding-related concern relating to staff misuse of technology, they should be report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's safeguarding and child protection policy.

Misuse by any user

Anyone who has a concern about the misuse of technology by any other user should report it immediately to the IT coordinator, the Designated Safeguarding Lead, or the Head.

The School reserves the right to withdraw access to the School's network by any user at any time and to report suspected illegal activity to the police.

If the School considers that any person is vulnerable to radicalisation the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

10 **Education**

The safe use of technology is integral to the School's curriculum. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices.

Technology is included in the educational programmes followed in the EYFS in the following ways:

- Children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;
- Children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and
- Children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

The safe use of technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies, PSHE and tutorial / pastoral activities, teaching pupils:

- about the risks associated with using the technology and how to protect themselves and their peers from potential risks;
- to be critically aware of content they access online and guided to validate accuracy of information;
- how to recognise suspicious, bullying or extremist behaviour;

- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- relevant laws applicable to the internet
- the consequences of negative online behaviour; and
- how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

The safe use of technology aspects of the curriculum are reviewed on a regular basis to ensure their relevance.

- The school uses PurpleMash to teach Computing in all age groups.
- The children from KG – Form 6 have their own username and password.
- PurpleMash is fully GDPR compliant.
- The IT coordinator has access to all staff and pupil PurpleMash accounts.

The School's acceptable use policy of ICT for pupils sets out the School rules about the use technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy on a regular basis.

Useful online safety resources for pupils

http://www.thinkuknow.co.uk/
http://www.childnet.com/young-people
https://www.saferinternet.org.uk/advice-centre/young-people
https://www.disrespectnobody.co.uk/
http://www.safetynetkids.org.uk/

11 **Training**

Staff

The School provides training on the safe use of technology to staff so that they are aware of how to protect pupils and themselves from the risks of using technology and to deal appropriately with incidents involving the use of technology when they occur.

Induction training for new staff will include training on the School's online safety strategy including this policy, the code of conduct and acceptable use of IT policy for staff. Ongoing staff development training includes training on technology safety together with specific safeguarding issues including sexting, cyberbullying and radicalisation.

Staff also receive GDPR training on induction and at regular intervals afterwards.

The frequency, level and focus of all such training will depend on individual roles and requirements and will be provided as part of the School's overarching approach to safeguarding.

Useful online safety resources for staff

(a) http://swgfl.org.uk/products-services/esafety

(b) https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals

(c) http://www.childnet.com/teachers-and-professionals

(e) https://www.thinkuknow.co.uk/teachers/

(f) http://educateagainsthate.com/

(g) https://www.commonsense.org/education/

(h) Cyberbullying: advice for head teachers and school staff (DfE, November 2014)

(i) Advice on the use of social media for online radicalisation (DfE and Home Office, July 2015)

(j) Sexting in schools and colleges: responding to incidents and safeguarding young people (UK Council for Child Internet Safety (UKCCIS), August 2016).

(k) Online safety in schools and colleges: questions from the governing board (UKCCIS, 2016)

(l) Education for a connected world framework (UKCCIS)

(m) Professionals online safety helpline: helpline@saferinternet.org.uk,

0344 381 4772.

The School works closely with parents to ensure they can safeguard their children whilst using technology. Information is regularly sent through the newsletter and via talks for parents. Parents are also advised upon best practice and introduced to current trends during Curriculum Information Evenings.

Parents are encouraged to read the acceptable use of ICT policy for pupils with their son / daughter to ensure that it is fully understood.

Useful online safety resources for parents

(a) https://www.saferinternet.org.uk/advice-centre/parents-and-carers

(b) http://www.childnet.com/parents-and-carers

(d) https://www.thinkuknow.co.uk/parents/

(e) http://parentinfo.org/

(f) http://parentzone.org.uk/

(g) https://www.net-aware.org.uk

(h) https://www.internetmatters.org/

(i) https://www.commonsensemedia.org/

12 **Record keeping**

All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

All serious incidents involving the use of technology will be logged centrally in the technology incident log by the IT coordinator and as part of the pupil or staff record.

The records created in accordance with this policy may contain personal data. The School has a number of privacy notices which explain how the School will use personal data about pupils and parents. The privacy notices are published on the School's website. In addition, staff must ensure that they follow the School's data protection policies and procedures when handling personal data created in connection with this policy. This includes the School's data protection policy and information security and sharing data guidance, which are contained in the Data Protection and Information Security Handbook.

13 **Version control**

The St Wystan's School Online safety policy

REVIEW
This policy will be reviewed on a two year rolling programme.

Written by:	Alistair Wolff		
Date Reviewed	January 2019 / January 2021		
Date of Next Review	January 2023		
Governing Body Approval	**Yes**/No	Signed/Dated	
Website/App	**Yes**/No	ISI	**Yes**/No
Staff Handbook	**Yes/**No	Parent Handbook	**Yes/**No