Policy Owner	M Shute
Approving Body	Board of Governors
Date Approved	February 2023
Effective Date	February 2023
Review date	February 2024

Online Safety Policy

St Aubyn's School

Contents

1 Aims

1.1 This is the online safety policy of St Aubyn's School.

1.2 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:

1.2.1 protects the whole School community from illegal, inappropriate and harmful content or contact;

1.2.2 educates the whole School community about their access to and use of technology; and

1.2.3 establishes effective mechanisms to identify, intervene and escalate incidents where appropriate.

1.2.4 creates a culture of safety, equality and protection.

2 Scope and application

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

2.2 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.

3 Regulatory framework

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

3.1.1 Education (Independent School Standards) Regulations 2014;

3.1.2 Statutory framework for the Early Years Foundation Stage (DfE, March 2021);

3.1.3 Education and Skills Act 2008;

3.1.4 Children Act 1989;

3.1.5 Data Protection Act 2018 and General Data Protection Regulation (**GDPR**); and

3.1.6 Equality Act 2010.

3.2 This policy has regard to the following guidance and advice:

3.2.1 Keeping children safe in education (DfE, September 2022) (**KCSIE**);

3.2.2 Preventing and tackling bullying (DfE, July 2017);

3.2.3 Sharing nudes and semi-nudes advice for education settings working with children and young people (Department of Digital, Media, Culture & Sport and UK Council for Internet Safety, December 2020);

3.2.4 Prevent duty guidance for England and Wales (Home Office, July 2015);

3.2.5 Channel duty guidance: protecting vulnerable people from being drawn into terrorism (Home Office, April 2015);

3.2.6 Searching, screening and confiscation: advice for schools (DfE, January 2018).

3.2.7 Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February 2019)

3.2.8 Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance (DfE, February 2019)

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

3.3.1 acceptable use of IT for pupils policy;

3.3.2 staff IT acceptable use policy and staff social media policy;

3.3.3 child protection and safeguarding policy and procedures;

3.3.4 anti-bullying policy;

3.3.5 risk assessment policy;

3.3.6 staff code of conduct policy;

3.3.7 whistleblowing policy and procedures;

3.3.8 data protection policy;

4 Publication and availability

4.1 This policy is published on the School website.

4.2 This policy is available in hard copy on request.

5 Definitions

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

References to the **Proprietor** are references to the Board of Governors.

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**).

6 Responsibility statement and allocation of tasks

6.1 The Proprietor has overall responsibility for all matters which are the subject of this policy.

6.2 The Proprietor is required to ensure that all those with management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Proprietor's response to this duty.

6.3 To ensure the efficient discharge of its responsibilities under this policy, the Proprietor 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	M Shute - Designated Safeguarding Lead (DSL) and Deputy Head	As required, and at least annually
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), relevant risk assessments and any action taken in response and evaluating effectiveness	M Shute - DSL and Deputy Head	As required, and at least termly
Online safety	M Shute – DSL and Deputy Head	
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the GDPR	M Shute – DSL and Deputy Head	As required, and at least termly
Formal annual review	Proprietor	Annually

7 Role of staff and parents

7.1 Headmaster and Senior Management Team

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

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

7.1.3 The DSL will work with the IT Team (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.

7.1.4 The DSL will regularly monitor the technology incident log maintained by Smoothwall.

7.1.5 The DSL will regularly update other members of the SMT on the operation of the School's safeguarding arrangements, including online safety practices.

7.2 IT Team

7.2.1 The IT Team, is 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.

7.2.2 The IT Team is responsible for ensuring that:

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

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

(c) the School has an effective filtering policy in place and that it is applied and updated on a regular basis;

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

(e) 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; and

(f) monitoring software (Smoothwall) and systems are kept up to date to allow the ICT team to monitor the use of School devices and the use of email and the internet over the School's network and maintain logs of such usage.

7.2.3 The School uses Smoothwall to filter and monitor inappropriate content and uses email to alert the DSL and Head to any safeguarding issues.

7.2.4 The IT Team will report regularly to the SMT on the operation of the School's technology. If the IT Team has concerns about the functionality, effectiveness, suitability or use of technology within the School, including of the monitoring and filtering systems in place, he / she will escalate those concerns promptly to the DSL.

7.3 **All staff**

7.3.1 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.

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

7.3.3 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 child protection policy. Staff are required to complete and submit to the DSL a Child Protection Initial Concern Form using the School’s Child Protection Online Management System (CPOMS) as soon as possible and within no more than 24 hours after any safeguarding incident relating to online safety.

7.4 **Parents**

7.4.1 The role of parents in ensuring that pupils understand how to stay safe when using technology is crucial. 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;

(d) follow the procedures in the Remote Learning Policy.

7.4.2 If parents have any concerns or require any information about online safety, they should contact the class teacher.

8 Access to the School's technology

8.1 The School provides internet and an email system to staff as well as other technology. Pupils and staff must comply with the respective acceptable use policy when using School technology. All such use is monitored by Smoothwall.

8.2 Pupils and staff require individual user names and passwords to access the School's internet and staff 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 team immediately.

8.3 No laptop or other mobile electronic device may be connected to the School network without the consent of an ICT Technician or the Network Manager. The use of any device connected to the School's network will be logged and monitored by the IT team. See also 8.5 below.

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

8.5 **Use of mobile electronic devices**

8.5.1 The School has appropriate filtering and monitoring systems in place to protect pupils using the internet when connected to the School's network.

8.5.2 The rules about the use of mobile electronic devices, including access to open / non-School networks, are set out in the acceptable use policy for pupils.

8.5.3 The use of mobile electronic devices by staff is covered in the Staff Code of Conduct, Staff IT Acceptable Use Policy, Staff Social Media Policy and Data Protection Policy. Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.

8.5.4 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

9.1 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, if applicable.

9.2 **Misuse by pupils**

9.2.1 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.

9.2.2 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 child protection and safeguarding policy).

9.3 **Misuse by staff**

9.3.1 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.

9.3.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they should 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 child protection policy.

9.4 **Misuse by any user**

9.4.1 Anyone who has a concern about the misuse of technology by any other user should report it immediately to the Designated Safeguarding Lead.

9.4.2 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.

9.4.3 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

10.1 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.

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

10.2.1 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;

10.2.2 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

10.2.3 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.

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

10.3.1 about the risks associated with using the technology and how to protect themselves and their peers from potential risks;

10.3.2 to be critically aware of content they access online and guided to validate accuracy of information;

10.3.3 how to recognise suspicious, bullying or extremist behaviour;

10.3.4 the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;

10.3.5 the consequences of negative online behaviour; and

10.3.6 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.

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

10.5 The School's Acceptable Use of IT for Pupils Policy sets out the School rules about the use of technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are regularly reminded of the importance of safe internet use.

10.6 **Useful online safety resources for pupils**

10.6.1 http://www.thinkuknow.co.uk/

10.6.2 http://www.childnet.com/young-people

10.6.3 https://childnet.com/resources/smartie-the-penguin

10.6.4 [https://www.childnet.com/resources/digiduck-stories

10.6.5 https://www.saferinternet.org.uk/advice-centre/young-people

10.6.6 https://www.disrespectnobody.co.uk/

10.6.7 http://www.safetynetkids.org.uk/

10.6.8 https://www.ceop.police.uk/Safety-Centre/How-can-CEOP-help-me-YP/

10.6.9 https://www.bbc.com/ownit

11 Training

11.1 Staff

11.1.1 The School provides training on the safe use of technology to relevant 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.

11.1.2 Induction training for new staff includes training on the School's online safety strategy including this policy, the staff code of conduct, staff IT acceptable use policy and social media policy. Ongoing staff development training during INSET and internal meeting time includes training on technology safety together with specific safeguarding issues including sexting, cyberbullying and radicalisation. All staff who supervise children using ICT are required to complete online e-safety training every two years. Staff also receive data protection training on induction and at regular intervals afterwards.

11.1.3 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.

11.1.4 **Useful online safety resources for staff**

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

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

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

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

(e) http://educateagainsthate.com/

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

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

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

(i) Sharing nudes and semi-nudes advice for education settings working with children and young people (Department of Digital, Media, Culture & Sport and UK Council for Internet Safety, December 2020);Online safety in schools and colleges: questions from the governing board (UKCCIS, 2016)

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

(k) https://www.lgfl.net/online-safety/resource-centre

(l) Online Sexual Harassment: Understand, Prevent and Respond Guidance for Schools (Childnet, March 2019)

(m) Myth vs Reality: PSHE toolkit (Childnet, April 2019)

(n)

(o) Professionals online safety helpline: helpline@saferinternet.org.uk, 0344 381 4772.

(p) NSPCC helpline for anyone worried about a child - 0808 800 5000

(q) Internet Watch Foundation - internet hotline for the public and IT professionals to report potentially criminal online content

11.2 Parents

11.2.1 The School believes that it is essential for parents to be fully involved with promoting online safety both in and outside of school. The School regularly communicates re online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage.

11.2.2 The School issues a monthly e-safety newsletter to parents and further advice is included in the fortnightly newsletter from the Head. Members of SMT cover this topic at general parents' evenings.

11.2.3 Parents are encouraged to read the acceptable use policy for pupils. Staff go through the acceptable use procedure for pupils in Years 3-8 at the start of each academic year.

11.2.4 **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

(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

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

(e) http://parentinfo.org/

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

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

(h) Advice for parents and carers on cyberbullying (DfE, November 2014).

(i) http://www.askaboutgames.com

(j) https://www.ceop.police.uk/safety-centre

12 UK CMO commentary on screen time and social media map of reviewsRisk assessment

12.1 Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified.

12.2 The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate). Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

12.3 The Bursar has overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

12.4 Day to day responsibility to carry out risk assessments under this policy will be delegated to the IT Team and the DSL,

13 Record keeping

13.1 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.

13.2 All incidents involving the use of technology are logged centrally in the technology incident log by Smoothwall and on a scale from 1 to 5 with 5 being the most serious.

13.3 The records created in accordance with this policy may contain personal data. The School has a 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 policies and procedures when handling personal data created in connection with this policy. This includes the School's data protection policy.