| | |
|---|---|
| Policy Owner | Deputy Head (Pastoral) |
| Approving Body | Board of Governors |
| Date Approved | Feb 2025 |
| Effective Date | Feb 2025 |
| Review date | Feb 2026 |

# Digital Policy (including Acceptable Use of IT Policy for Pupils and Online Safety Policy)

## St. Aubyn's School

**Contents**

**Digital Policy for St. Aubyn's School**

**Introduction**

*'Education should prepare young people for jobs that do not yet exist, using technologies that have not yet been invented, to solve problems of which we are not yet aware.' Richard Riley (no date).*

At St. Aubyn's, we recognize the importance of digital technologies in today's world and their potential to enhance the learning experience for our pupils. This Digital Policy outlines our commitment to providing a safe and responsible digital learning environment for pupils from Nursery to Year 6. Our goal is to empower pupils to become responsible digital citizens while ensuring their safety and privacy.

Digital technologies are, and will continue to be a focus in our SIP.

**Purpose**

The purpose of this Digital Policy is to:

1. Promote responsible and safe use of digital technologies.
2. Promote digital learning and digital literacy across the school
3. Protect the privacy and security of pupils and staff.
4. Provide guidelines for the integration of digital technologies into the curriculum.
5. Ensure compliance with relevant laws and regulations.
6. Outline the responsibilities of staff and pupils concerning AI usage in School.

**Responsible Use of Digital Technologies**

**Pupil Responsibilities**

1. Pupils are expected to use digital devices and online resources in a responsible and respectful manner, in accordance with the Acceptable Use of IT Policy (page 6).
2. Pupils should report any inappropriate or harmful online behaviour to a teacher or staff member.
3. Pupils must not share personal information, such as full names, addresses, or contact details, online without permission from a parent or guardian.

**Parent/Guardian Responsibilities**

1. Parents and guardians are encouraged to monitor their child's online activities and communicate with the school regarding any concerns.
2. Parents and guardians should support their child in following the school's digital policies and guidelines.

**Staff Responsibilities**

1. Staff are expected to use digital devices and online resources in a responsible and respectful manner, in accordance with staff policies including the Staff Social Media Policy and the Staff IT Acceptable Use Policy.
2. Staff members must model responsible digital behaviour for pupils.
3. Staff members should educate pupils about online safety and responsible use of digital technologies.

**Online Safety**

1. All members of the School community are expected to behave in accordance with the Online Safety Policy (page 25).
2. We will implement filtering and monitoring systems to block inappropriate content and websites on school devices.
3. Pupils will receive guidance on how to protect their personal information and stay safe online.
4. Cyberbullying and inappropriate online behaviour will not be tolerated, and appropriate consequences will be enforced.

**Digital Learning and Digital Literacy**

1. We aim for learners to experience opportunities to develop their digital literacy across all curricular areas, using a range of digital tools and applications.
2. We aspire to use digital technology to enrich our teaching and learning across all areas of the curriculum.
3. We aim to equip our children and young people with the vital digital skills needed to adapt in our ever-changing technological society.

**Privacy and Data Protection**

1. The school will collect and store pupil data in accordance with relevant data protection laws, such as the General Data Protection Regulation (GDPR).
2. Parents and guardians will be informed about the types of data collected and how it will be used.
3. Only authorized personnel will have access to pupil data, and it will be used solely for educational purposes.

**Digital Curriculum Integration**

1. Digital technologies will be integrated into the curriculum to enhance learning experiences.
2. Teachers will receive professional development to effectively use digital tools in the classroom.
3. The school will provide access to age-appropriate digital resources and software.

**Compliance with Laws and Regulations**

1. The school will comply with all relevant laws and regulations related to digital technology use in educational settings.
2. Any concerns or complaints related to digital technology use should be reported to the school's designated responsible officer.

**Review and Revision**

This Digital Policy will be reviewed annually to ensure its effectiveness and relevance. Any necessary revisions will be made to adapt to changing technologies and educational needs.

St. Aubyn's is committed to providing a safe, responsible, and enriching digital learning environment for our pupils. We believe that with the right guidance and support, pupils can harness the power of digital technologies for their educational benefit while staying safe and respectful online.

L. Taylor

St. Aubyn's School

February 2025

# Acceptable Use of IT Policy for Pupils

**Contents**



**Appendix**

## 1 Aims

1.1 This is the acceptable use policy for pupils of St Aubyn's School.

1.2 The aims of this policy are as follows:

1.2.1 to educate and encourage pupils to make good use of the educational opportunities presented by access to technology;

1.2.2 to safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:

(a) exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials);

(b) the sharing of personal data, including images;

(c) inappropriate online contact or conduct; and

(d) cyberbullying and other forms of abuse.

1.2.3 to minimise the risk of harm to the assets and reputation of the School;

1.2.4 to help pupils take responsibility for their own safe use of technology;

1.2.5 to ensure that pupils use technology safely and securely and are aware of both external and peer-to-peer risks when using technology;

1.2.6 to prevent the unnecessary criminalisation of pupils; and

1.2.7 to help to create 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 pupils accessing the School's technology whether on or off School premises, or using their own or others' technology in a way which affects the welfare of pupils or any member of the School community or where the culture or reputation of the School is put at risk.

2.3 Appendix 6 has a pupil friendly version of the procedures in this policy. Staff go through these with Year 3 to 6 pupils at the start of each term and younger pupils are told them in terms that are appropriate to their understanding and use of IT. The School actively promotes the participation of parents to help the School safeguard the welfare of pupils and promote the safe use of technology.

## 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 2014, updated September 20);

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 2024) (**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 (DfSI&T, Updated March 2024)

3.2.4 How can we stop prejudice based bullying in schools? (Equality and Human Rights Commission);

3.2.5 Sexual violence and sexual harassment between children in schools and colleges (DfE, December 2017, updated September 2021);

3.2.6 Searching, screening and confiscation: advice for schools (DfE, July 2022);

3.2.7 Safeguarding children and protecting professionals in early years settings: online safety considerations (UK Council for Internet Safety, February2019); and

3.2.8 Relationships education, relationships and sex education and health education guidance (DfE, June 2019).

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

3.3.1 behaviour management policy;

3.3.2 anti-bullying policy;

3.3.3 online safety policy;

3.3.4 child protection and safeguarding policy;

3.3.5 risk assessment 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.

4.3 This policy can be made available in large print or other accessible format if required.

## 5 Definitions

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

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

5.2 The School will take a wide and purposive approach to considering what falls within the meaning of **technology**. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including:

5.2.1 the internet;

5.2.2 email;

5.2.3 mobile phones and smartphones;

5.2.4 wearable technology;

5.2.5 desktops, laptops, netbooks, tablets / phablets;

5.2.6 personal music players;

5.2.7 devices with the capability for recording and / or storing still or moving images;

5.2.8 social networking, micro blogging and other interactive websites;

5.2.9 instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards;

5.2.10 webcams, video hosting sites (such as YouTube);

5.2.11 gaming sites;

5.2.12 virtual learning environments such as VLe;

5.2.13 SMART boards; and

5.2.14 other photographic or electronic equipment e.g. GoPro devices.

## 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 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 | Designated Safeguarding Lead | As required, and at least annually |
| Monitoring the use of technology across the School, maintaining appropriate logs and reviewing the policy to ensure that it remains up to date with technological change | Designated Safeguarding Lead | 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 | Designated Safeguarding Lead | As required, and at least annually |

| Task | Allocated to | When / frequency of review |
|---|---|---|
| Online safety | Designated Safeguarding Lead | As required, and at least annually |
| Maintaining up to date records of all information created in relation to the policy and its implementation as required by the GDPR | Designated Safeguarding Lead | As required, and at least annually |
| Formal annual review | Proprietor | Annually |

## 7 Safe use of technology

7.1 We want pupils to enjoy using technology and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.

7.2 The School will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of our systems. The safe use of technology is integral to the School's curriculum. Pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

7.3 Pupils may find the following resources helpful in keeping themselves safe online:

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

7.3.2 https://www.childnet.com/young-people

7.3.3 https://www.childnet.com/resources/smartie-the-penguin

7.3.4 https://www.childnet.com/resources/digiduck-stories

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

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

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

7.3.8 http://www.childline.org.uk/Pages/Home.aspx

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

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

7.4 Please see the School's online safety policy (page 25) for further information about the School's online safety strategy.

## 8 Internet and email

8.1 The School provides internet access to pupils to support their academic progress and development.

8.2 Pupils may only access the School's network when given specific permission to do so. All pupils will receive guidance on the use of the School's internet systems. If a pupil is unsure

about whether they are doing the right thing, they must seek assistance from a member of staff.

8.3 For the protection of all pupils, their use of the internet will be monitored by the School. Pupils should remember that even when something that has been downloaded or has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private.

8.4 The School uses the filters and monitoring tools in Smoothwall to keep pupils safe.

## 9 IT Procedures and Principles

9.1 Pupils **must** comply with the following procedures and principles:

9.1.1 access and security (Appendix 1);

9.1.2 use of internet and email (Appendix 2);

9.1.3 use of mobile electronic devices (Appendix 3); and

9.1.4 photographs and images (including "sexting") (Appendix 4).

9.2 The purpose of these rules is to set out the principles which pupils must bear in mind at all times and also the rules which pupils must follow to use technology safely and securely.

9.3 These principles and rules apply to all use of technology.

## 10 Procedures

10.1 Pupils are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If a pupil is aware of misuse by other pupils they should talk to a teacher about it as soon as possible.

10.2 Any misuse of technology by pupils will be dealt with under the School's behaviour management policy and where safeguarding concerns are raised, under the safeguarding child protection policy and procedures.

10.3 Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's anti-bullying policy. If a pupil thinks that he / she might have been bullied or that another person is being bullied, he / she should talk to a teacher about it as soon as possible. See the School's anti-bullying policy for further information about cyberbullying and e-safety, including useful resources.

10.4 The Designated Safeguarding Lead takes lead responsibility within the School for safeguarding and child protection, including online safety. In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's child protection and safeguarding policy and procedures).

10.5 If a pupil is worried about something that he / she has seen on the internet, or on any electronic device, including on another person's electronic device, he / she must tell a teacher about it as soon as possible.

10.6 In a case where the pupil is considered to be vulnerable to radicalisation they may be referred to the Channel programme. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

10.7 In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead who will record the matter centrally in the technology incidents log.

## 11 Sanctions

11.1 Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the Proprietor has authorised the Head to apply any sanction which is appropriate and proportionate to the breach in accordance with the School's behaviour management policy including, in the most serious cases, expulsion. Other actions might include: increased monitoring procedures and withdrawal of the right to access the School's internet facilities. Any action taken will depend on the seriousness of the offence.

11.2 Unacceptable use of technology could lead to the confiscation of a device or deletion of the material in accordance with the procedures in this policy and the School's behaviour management policy.

11.3 If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence e.g. upskirting, or that it contains a pornographic image of a child or an extreme pornographic image, the device will be given to the police. See Appendix 4 for more information on photographs and images.

11.4 The School reserves the right to charge a pupil or their parents for any costs incurred to the School as a result of a breach of this policy.

## 12 Training

12.1 The School ensures that regular guidance and training is arranged on induction and at regular intervals thereafter so that staff and volunteers understand what is expected of them by this policy and have the necessary knowledge and skills to carry out their roles.

12.2 The level and frequency of training depends on role of the individual member of staff.

12.3 The School maintains written records of all staff training.

## 13 Risk assessment

13.1 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.

13.2 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.

13.3 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.

13.4 Day to day responsibility to carry out risk assessments under this policy will be delegated to the Deputy Head

## 14 Record keeping

14.1 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.

14.2 All serious incidents involving the use of technology will be logged centrally in the technology incident log by Smoothwall and dealt with by the Designated Safeguarding Lead.

14.3 The records created in accordance with this policy may contain personal data. The School has a privacy notice which explains how the School will use personal data about pupils and parents. The privacy notice is published on the School's website. In addition, staff must ensure that they follow the School's data protection policy when handling personal data created in connection with this policy.

## Appendix 1

## Access and security

1 Access to the internet from the School's computers and network must be for educational purposes only. You must not use the School's facilities or network for personal, social or non-educational use.

2 You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.

3 No laptop or other mobile electronic device may be connected to the School network during school hours without the consent of a member of staff.

4 The use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while you are on School premises or otherwise in the care of the School is strictly prohibited at all times.

5 Passwords protect the School's network and computer system. You must not let anyone else know your password. If you believe that someone knows your password you must change it immediately.

6 You must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you are not authorised to access. If there is a problem with your passwords, you should speak to your class teacher.

7 You must not attempt to access or share information about others without the permission of a member of staff. To do so may breach data protection legislation and laws relating to confidentiality.

8 The School has a firewall in place to ensure the safety and security of the School's networks. You must not attempt to disable, defeat or circumvent any of the School's security facilities. Any problems with the firewall must be reported to the class teacher or ICT technician. Please see Appendix 5 for further information regarding the use of iPads.

9 The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. You must not try to bypass this filter.

10 Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If you think or suspect that an attachment, or other downloadable material, might contain a virus, you must speak to the ICT technician before opening the attachment or downloading the material.

11 You must not disable or uninstall any anti-virus software on the School's computers.

12 The use of location services represents a risk to the personal safety of pupils and to School security. The use of any website or application, whether on a School or personal device, with the capability of identifying the user's location while you are on School premises or otherwise in the care of the School is strictly prohibited at all times.

## Appendix 2

## Use of the internet and email

1 The School does not undertake to provide continuous internet access. Email and website addresses at the School may change from time to time.

**Use of the internet**

2 You must use the School's computer system for educational purposes only and are not permitted to access interactive or networking websites without the express, prior consent of a member of staff.

3 You must take care to protect personal and confidential information about yourself and others when using the internet, even if information is obtained inadvertently. You should not put personal information about yourself, for example your full name, address, date of birth or mobile number, online.

4 You must not load material from any external storage device brought in from outside the School onto the School's systems, unless this has been authorised by a teacher.

5 You should assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights - you must not copy (plagiarise) another's work.

6 You must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. You must tell a member of staff immediately if you have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

7 You must not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.

8 You must not bring the School into disrepute through your use of the internet.

**Use of email**

9 You must not use any personal web-based email accounts such as Gmail, Yahoo or Hotmail through the School's network without the express, prior consent of a teacher.

10 Email should be treated in the same way as any other form of written communication. You should not include or ask to receive anything in an email which is not appropriate to be published generally or which you believe the Head and / or your parents would consider to be inappropriate. Remember that emails could be forwarded to or seen by someone you did not intend.

11 You must not send or search for any email message which contains offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If you are unsure about the content of a message, you must speak to a member of staff. If you come across such material you must

inform a member of staff as soon as possible. Use of the email system in this way is a serious breach of discipline and may constitute a criminal offence.

12 Trivial messages and jokes should not be sent or forwarded through our email system. These could cause distress to recipients (if considered to be inappropriate).

13 You must not read anyone else's emails without their consent.

## Appendix 3

## Use of mobile electronic devices

1 **Mobile electronic device** includes but is not limited to mobile phones, smartphones, tablets, laptops and MP3 players.

2 Mobile phones and other mobile electronic devices should not be brought to School by pupils with the exception of Year 6 pupils, who may bring in a mobile phone if they travel independently.

3 Year 6 Pupils who bring their mobile phone to school must have it switched off and placed in their locker from their first arrival at school. It must not be kept in their bag.

4 The use of cellular data (e.g. GPRS, 3G, 4G, etc) to access the internet while you are on School premises or otherwise in the care of the School is strictly prohibited at all times.

5 The use of mobile phones by pupils during the School dayand/or on the School site is not allowed. In emergencies, you may request to use the School telephone. Should your parents wish to contact you in an emergency, they will telephone the School office and a message will be relayed promptly.

6 You must not communicate with staff using a mobile phone (or other mobile electronic device) under any circumstances.

7 Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not you are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's anti-bullying policy and behaviour management policy) and the School's safeguarding procedures will be followed in appropriate circumstances (see the School's child protection and safeguarding policy and procedures).

8 Mobile electronic devices may be confiscated and searched in appropriate circumstances. Please see the School's behaviour management policy. You may also be prevented from bringing a mobile electronic device into the School temporarily or permanently and at the sole discretion of the Head.

9 The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff.

## Appendix 4

## Photographs and images

1 Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

2 You may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image. If the material found is a pornographic image of a child or an extreme pornographic image this will not be deleted and the device will be delivered to the police, as stated in paragraph 11.3 of this policy.

3 If material found on a device is a still or moving image that has been obtained by 'upskirting' this will not be deleted and the device will be delivered to the police, as stated in paragraph 11.3 of this policy.

4 You must allow staff access to images stored on mobile phones and / or cameras and must permanently delete images if requested to do so.

5 The posting of images which in the reasonable opinion of the Head is considered to be offensive or which brings the School into disrepute on any form of social media or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

6 **Sexting**

6.1 **Sexting** means the taking and sending or posting of images or videos of a sexual or indecent nature of you or another pupil, usually through mobile picture messages or webcams over the internet.

6.2 Sexting is strictly prohibited, whether or not you are in the care of the School at the time the image is recorded and / or shared.

6.3 Sexting may be a criminal offence, even if the picture is taken and shared with the permission of the person in the image. Even if you are not prosecuted, this may result in information being stored on your police record, which may prevent you from doing certain jobs in the future.

6.4 The police may seize any devices which they believe may have been used for sexting. If the police find that a device contains inappropriate images, they are unlikely to return it to you.

6.5 Remember that once a photo or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied and may be shared by others.

6.6 Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.

6.7 Even if you don't share images yourself, there is a risk that you may lose your device, it may be "hacked", or its data may still be accessible to a future owner.

6.8 The School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection and safeguarding policy and procedures.

6.9 If you are concerned about any image you have received, sent or forwarded or otherwise seen, speak to any member of staff for advice.

6.10 If sexual images or videos have been made and circulated online, you can be supported to get the images removed through the Internet Watch Foundation.

## 7 Upskirting

7.1 Upskirting typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing parts of their body or clothing, not otherwise visible, to obtain sexual gratification, or cause the victim humiliation, distress or alarm.

7.2 Upskirting is strictly prohibited, whether or not you are in the care of the School at the time the image is recorded.

7.3 Upskirting is a criminal offence. Attempting to commit an act of upskirting may also be a criminal offence e.g. if actions are taken to do something that is more than merely preparatory to committing the offence such as attempting to take a photograph on a telephone or camera but failing to do so because of lack of storage space or battery.

7.4 The School will treat incidences of upskirting as a breach of discipline and also as a safeguarding matter under the School's child protection and safeguarding policy and procedures.

7.5 If you are concerned that you have been a victim of upskirting, speak to any member of staff for advice.

8

**Appendix 5**

iPad Responsible Use Procedures for St Aubyn's Prep School Pupils

The information within this document applies to all iPads used in school. Please note that the Acceptable Use of IT Policy for Pupils also applies to all iPad use. Teachers and other school staff may set additional requirements for use within their classroom.

User Responsibilities

- Users must not remove the protective case from their iPad. The iPad screen is made of glass and therefore is subject to cracking and breaking if misused. Never drop or place heavy objects (books, laptops, etc.) on top of the iPad.
- Only a soft cloth is to be used to clean the iPad screen.
- Do not subject the iPad to extreme heat or cold.
- Do not store anywhere other than in a ***padlocked*** locker or the classroom charging unit.
- Users may not photograph or film any other person without that persons' consent and only when directed to by a teacher.
- The iPad is subject to routine monitoring by St Aubyn's School.
- Devices must be surrendered immediately upon request by any member of staff.
- Users in breach of the Responsible Use Procedures may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

Additional Responsibilities for Pupils

- Pupils must not use their iPad in school corridors, changing rooms or outside of school buildings (unless with the teachers' permission).

Safeguarding and Maintaining as an Academic Tool

- iPad batteries are required to be charged and be ready to use in school.
- Syncing the iPad to iTunes or iCloud will be maintained by a School administrator.
- Items deleted from the iPad cannot be recovered. Memory space is limited. Academic content takes precedence over personal files and apps.
- The whereabouts of the iPad should be known at all times. ***It is a user's responsibility to keep their iPad safe and secure.***
- iPads belonging to other users are not to be tampered within any manner.
- If an iPad is found unattended, it must be given to the nearest member of staff.

Lost, Damaged or Stolen iPad

- If the iPad is lost, stolen, or damaged, the Head of Senior School must be notified immediately.
- iPads that are believed to be stolen can be tracked through iCloud.

Prohibited Uses (not exclusive):

- Accessing Inappropriate Materials – All material on the iPad must adhere to the Acceptable Use of IT Policy for Pupils.
- Users are not allow to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- Violating Copyrights – Users are not allowed to have music and install apps on their iPad.

Cameras

- Users must use good judgment when using the camera.
- The user agrees that the camera will not be used to take inappropriate, illicit or explicit photographs or videos, nor will it be used to embarrass anyone in any way.
- Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation.
- Images of other people may only be used with the permission of those in the photograph.
- Posting of images/movie on the internet into a public forum is strictly forbidden, without the express permission of the teacher.
- Use of the camera and microphone is strictly prohibited, unless express permission is granted by a teacher.

Misuse of Passwords, Codes or other Unauthorised Access -

- Any user caught trying to gain access to another user's accounts, files or data will be subject to sanctions.

Malicious Use/Vandalism –

- Any attempt to destroy hardware, software or data will be subject to disciplinary action.

Jailbreaking –

- Jailbreaking is the process of which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.
- Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.
- Users should be aware of and abide by the guidelines set out by in this Responsible Use Procedures.
- St Aubyn's School reserves the right to confiscate and search an iPad to ensure compliance with this Responsible Use Procedures.

**Pupil Pledge for iPad Use**

**This pledge will be shared and discussed at the beginning of each term by Form Tutors**

- I will take good care of my iPad.
- I will never leave the iPad unattended. If it is not with me in a lesson, it ***must*** be secured in a padlocked locker.
- I will know where my iPad is at all times.
- I will charge my iPad's battery at the end of every school day by returning it to the charging unit at 4.00pm.
- I will keep food and drinks away from my iPad since they may cause damage to the device.
- I will not disassemble any part of my iPad or attempt any repairs.
- I will use my iPad in ways that are appropriate.
- I understand that my iPad is subject to inspection at any time without notice.
- I will only photograph and use photographs of people with their permission and when directed by a teacher.
- I will only use the camera or the microphone when my teacher tells me to.
- I will never share any images or movies of people in a public space on the internet, unless I am asked to do so by a teacher.
- If my own actions result in the loss, theft or damage of an iPad then I may be responsible for the cost of repair or replacement
- I agree to abide by the statements of the Responsible Use Procedures

**Appendix 6 St. Aubyn's Pupil IT Acceptable Use Procedures (AUP)**

New technologies have become integral to the lives of young people in today's society, both within school and in their lives outside school. The internet and other digital information technologies are powerful tools, which open up new opportunities for everyone. Young people should have an entitlement to safe internet access at all times.

The School has a network of computers, tablets and other devices with internet access to help teaching and learning. This AUP also applies to devices that senior pupils bring into school, such as their mobile phone.

These procedures are intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other information technologies for educational, personal and recreational use.
- that School IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Normal school rules for behaviour apply when working with IT equipment (e.g. computers, iPads, cameras, etc.).

IT Equipment

- School IT systems are intended for educational use; pupils should only use the systems for recreational use rarely and only with the permission of their teacher.
- Do not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- Treat all IT equipment responsibly.
- Do not eat or drink in a computer room or near any IT equipment.
- Only use IT equipment for school work and homework.
- Do not print out homework on school printers or copiers.
- Do not install or attempt to install programs of any type on a school machine, or store programs on the school system, or try to alter school computer settings.
- Report any faults or damage to equipment immediately.

Logging In

- Only access the system with authorised login and passwords.
- Do not share your log in details, passwords etc. with others
- Do not use another person's login, password or access their files.
- Do not leave a computer logged on.
- Do not change or alter any computer settings.

Storage Devices

- Do not bring discs, memory sticks and other storage devices containing software i.e. programmes, games into school.
- Only use discs, memory sticks and other storage devices that have been scanned for viruses and have been permitted by staff to use.

Files may be deleted by IT staff if they are considered to be a security threat.

Child Protection/Safeguarding

- Only use the internet under supervision.
- Respect others' work and property; do not access, copy, remove, send or otherwise alter any other user's files, without the owner's knowledge and permission.
- Be polite and responsible when you communicate with others; do not use strong, aggressive or inappropriate language.
- Do not take or distribute images of anyone without their permission. This includes, but is not limited to, screenshots, photos and/or recordings of pupils and/or staff from social media, Nearpod lessons and conference calls (e.g. Zoom, Microsoft Teams, Google classroom etc)
- Do not use external email, messaging or social networking sites or contact people unless as part of a school-approved scheme.
- Do not download, send or share text, graphics, audio or video material which is offensive, upsetting, abusive, obscene or defamatory or which may be unlawful. Any unpleasant or inappropriate material or messages received must be reported immediately.
- Do not disclose or share personal information e.g. home address, telephone number or any other contact information or arrange to meet anyone through the internet.
- Do not open any attachments to emails, unless you know and trust the person or organisation that sent the email, due to the risk of the attachment containing viruses or other harmful programs
- Report any accessing (deliberate or intentional) of inappropriate material. These reports will be confidential and will help to protect other pupils.
- Do not access inappropriate websites and proxy servers to try and circumvent the School's filtering system.

School IT staff, the Deputy Head (admin) and the Head will be able to monitor individual use of IT systems, including internet sites visited, messages sent etc. Misuse of IT equipment and inappropriate activity will result in sanctions. This applies in school and to out of school use that involves members of the School community.

These rules will be explained to pupils from Year 3 to Year 6 at the start of each year. Younger pupils will be told in terms that are appropriate to their level of understanding and their use of IT equipment. Parents are expected to monitor carefully their children's use of IT equipment and to support these rules outside of school.

# Online Safety Policy

**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, November 2024);

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 2024) (**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, Updated March 2024);

3.2.4 Prevent duty guidance for England and Wales (Home Office, Updated March 2024);

3.2.5 Channel duty guidance: protecting people susceptible to radicalisation (Home Office, Updated December 2023);

3.2.6 Searching, screening and confiscation: advice for schools (DfE, July 2022).

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;

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 | 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 | Deputy Head | As required, and at least termly |
| Online safety | Deputy Head | |
| Maintaining up to date records of all information created in relation to the policy and its implementation as required by the GDPR | Deputy Head | As required, and at least termly |
| Formal annual review | Proprietor | Annually |

## 7 Role of staff and parents

### 7.1 Head 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 the ICT Technician. 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, Updated March 2024);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) Professionals online safety helpline: helpline@saferinternet.org.uk, 0344 381 4772.

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

(p) 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 3-6 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 reviews Risk 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.

# EdTech Strategy for St Aubyn's School

**Contents**

St Aubyn's School recognizes the transformative potential of educational technology (EdTech) to enhance teaching and learning experiences for our pupils. This EdTech Strategy outlines our commitment to integrating technology into our curriculum while ensuring its effective and responsible use. Our goal is to leverage EdTech to support our educational objectives, foster creativity, and prepare our pupils for a digital future.

St Aubyn's School is committed to harnessing the power of educational technology to provide our pupils with a high-quality, inclusive, and forward-thinking education. By implementing this EdTech Strategy, we aim to prepare our pupils for success in an increasingly digital world, while maintaining a focus on their well-being, safety, and holistic development.

1. **Vision and Goals**

**Vision**: To create a dynamic, inclusive, and technologically empowered learning environment that prepares our pupils for the challenges of the 21st century.

**Goals**:

1. **Enhanced Learning**: Utilize EdTech to enhance pupil engagement, critical thinking, and knowledge acquisition.
2. **Digital Literacy**: Equip pupils with digital literacy skills necessary for success in an increasingly technology-driven world.
3. **Inclusivity**: Ensure all pupils have equitable access to EdTech resources, regardless of their background or abilities.
4. **Professional Development**: Provide ongoing training and support for teachers to effectively integrate technology into their teaching practices.
5. **Data-Driven Decision-Making**: Use data from EdTech tools to inform instructional strategies and continuously improve learning outcomes.

**2. EdTech Integration**

**a. Curriculum Enhancement**

- Identify areas where EdTech can enhance the curriculum, aligning technology use with learning objectives.
- Collaborate with subject specialists and EdTech experts to develop and select digital content and resources that support the curriculum.

**b. Device Deployment**

- Ensure that all classrooms are equipped with appropriate digital devices, such as laptops or tablets, to facilitate digital learning.

**c. Digital Content**

- Invest in a diverse range of educational software, applications, and online resources that cater to different learning styles and abilities.
- Regularly update and evaluate the quality and suitability of digital content.

**d. Teacher Training**

- Provide comprehensive professional development opportunities for teachers to build their EdTech competencies.
- Foster a culture of continuous learning by encouraging teachers to explore new tools and share best practices.

**e. Digital Citizenship**

- Integrate lessons on digital citizenship, online safety, and responsible technology use into the curriculum.
- Encourage pupils to be ethical and responsible digital citizens both in and out of school.

**3. Access and Equity**

**a. Inclusivity**

- Ensure that all pupils have access to the necessary technology resources, regardless of their socio-economic background or special needs.
- Provide support and accommodations for pupils with disabilities to fully participate in digital learning.

**b. Connectivity**

- Collaborate with local authorities and internet service providers to improve internet connectivity in underserved areas.

**4. Data and Privacy**

**a. Data Security**

- Implement robust data security measures to protect pupil and staff data, adhering to GDPR regulations.
- Educate staff and pupils about data privacy and the responsible use of technology.

**b. Data Analytics**

- Collect and analyse data from EdTech tools to assess pupil progress, identify areas for improvement, and inform instructional decisions.
- Use data to personalize learning experiences and provide targeted support to pupils.

**5. Evaluation and Review**

- Conduct regular evaluations of the effectiveness of EdTech integration, seeking feedback from teachers, pupils, and parents.
- Make necessary adjustments to the EdTech strategy based on evaluation results and changing educational needs.

# The Use of AI in School

**Contents**

We recognise the importance of integrating Artificial Intelligence (AI) technologies into our educational practices. AI offers exciting opportunities to enhance learning experiences, streamline administrative tasks, and foster innovation. This policy outlines guidelines for pupils and staff to ensure the safe, ethical, and responsible use of AI within our school community.

**Purpose:**

1. Establish guidelines for the appropriate and responsible use of AI technologies within the school environment.
2. Ensure the safety, privacy, and well-being of pupils and staff when interacting with AI systems.
3. Foster a culture of digital citizenship, critical thinking, and ethical decision-making concerning AI technologies.

**Policy Guidelines:**

**i. Responsible Use:**

- Pupils and staff are expected to use AI technologies in a responsible manner, adhering to the school's code of conduct and ethical guidelines.
- AI tools should be utilised for educational purposes, research, and administrative tasks within the school context.

**ii. Privacy and Data Protection:**

- Pupils' and staff's privacy rights must be respected when using AI technologies. Personal data should only be collected, stored, and processed in accordance with relevant data protection laws (e.g., GDPR).
- Any data collected through AI systems should only be used for educational or administrative purposes and should not be shared with third parties without appropriate consent or legal justification.

**iii. Bias and Fairness:**

- Pupils and staff should be aware of the potential biases inherent in AI systems and strive to mitigate them.
- AI technologies should be used in a manner that promotes fairness, equity, and inclusivity, avoiding the perpetuation of stereotypes or discrimination based on race, gender, ethnicity, religion, disability, or any other characteristic.

**iv. Safety and Well-being:**

- AI tools should not be used in a manner that compromises the physical, emotional, or psychological safety of pupils or staff.
- Adequate safeguards should be in place to prevent harmful or inappropriate content from being accessed through AI systems.
- Any suspicious activities or security incidents involving AI technologies should be reported immediately to the school's IT department or designated personnel.

**v. Intellectual Property and Attribution:**

- Respect for intellectual property rights must be maintained when using AI-generated content or collaborating with AI tools.
- Proper attribution should be given to AI-generated work or contributions in accordance with copyright laws and academic integrity principles.

**vi. Training, Supervision and Support:**

- Adequate training and supervision and support should be provided to pupils and staff when using AI technologies, especially for younger pupils or those with limited digital literacy skills.
- Educational resources and guidelines will be made available to help users develop the necessary skills and knowledge to effectively utilize AI tools in their learning and work.

**vii. Reporting and Feedback:**

- Pupils and staff are encouraged to report any concerns, incidents, or issues related to the use of AI technologies promptly.
- This policy will be reviewed periodically to reflect changes in technology, legal requirements, and best practices.

**viii. Implementation:**

- The Head, along with the leadership team, is responsible for overseeing the implementation of this policy.
- Staff training sessions will be organized to familiarize teachers with the guidelines and best practices outlined in this policy.
- Regular reviews and updates to the policy will be conducted to ensure its relevance and effectiveness.