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

Acceptable Use of IT Policy for Pupils

St Aubyn's School

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 8 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 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 (DfDCMS, December 2020)

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, January 2018);

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 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 he / she is doing the right thing, he / she 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 he / she 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 Headmaster 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 sanctions might include: increased monitoring procedures; withdrawal of the right to access the School's internet and email facilities; detention. 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 his / her 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 Headmaster 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 that are handed in must be switched off (and not just on silent mode).

3 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.

4 The use of mobile phones during the School day will not be necessary. 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.

5 You must not communicate with staff using a mobile phone (or other mobile electronic device) except when this is expressly permitted by a member of staff, for example when necessary during an educational visit. Any such permitted communications should be brief and courteous.

6 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).

7 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 Headmaster.

8 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 Headmaster 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.

Appendix 5

iPad Responsible Use Procedure for St Aubyn's Senior 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 Policy 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 the Responsible Use Policy.
- St Aubyn's School reserves the right to confiscate and search an iPad to ensure compliance with this Responsible Use Policy.

Pupil Pledge for iPad Use

Users must read and sign below:

I have read, understand and agree to abide by the terms of the iPad Responsible Use Procedure

- 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 Policy

Name _____

Signature _____

Date _____

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 8 at the start of each year and sent to their parents. 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.