Policy Owner	Len Blom / Marcus Shute
Approving Body	Board of Governors
Date Approved	May 2017
Effective Date	May 2017
Review date	May 2018

E-Safety Policy

St Aubyn's (Woodford Green) School Trust

E-Safety Policy

Introduction

It is the duty of St Aubyn's School to ensure that every pupil in its care is safe and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, radicalisation and abuse.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable Use Procedures (AUP) (see Appendix) for staff and pupils, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At St Aubyn's School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

Both this policy and the AUP for staff and pupils cover both fixed and mobile internet devices provided by the School such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc., as well as all devices owned by pupils and staff brought onto school premises (personal laptops, tablets, smart phones, etc.).

Roles and responsibilities

The Designated Safeguarding Lead (DSL) and Head have responsibility for ensuring this policy is upheld by all members of staff. They will keep up to date on current e-safety issues and guidance issued by organisations such as the Local Authority, Child Exploitation and Online Protection (CEOP) Childnet International, the Local Authority Safeguarding Children Board and the Prevent Duty guidance. As with all issues of safety at the School, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis and this includes an awareness of material pupils may access on the internet

The statutory guidance makes clear the need for the School to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. The School has suitable filtering in place monitored by IT staff.

The School has an important role to play in equipping pupils to stay safe online, both in school and outside. Internet safety is integral to the School's ICT curriculum and is embedded in the ICT and PSHE curricula. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website, http://www.saferinternet.org.uk/

The School believes that it is essential for parents / carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents / carers and seek to promote a wide understanding of the benefits and risks related to internet usage.

Staff awareness

New teaching staff receive this e-Safety Policy and AUP as part of their induction. All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All staff who supervise children using ICT complete an online e-safety assessment every two years. Supply staff and contractors also receive our e-Safety Policy on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. These behaviours are summarised in the AUP which Year 3 -5 class teachers and senior tutors go through with the pupils on the first day of the School year. When children use school computers, staff will make sure children are fully aware of the contents of the AUP.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They will know what to do in the vent of misuse of technology by any member of the School community.

An Initial Concern Form must be completed by staff as soon as possible after any safeguarding incident relating to e-safety occurs and be given directly to the School's DSL within 24 hours of such an incident.

E-Safety in the curriculum and school community

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The School provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, as well as informally when opportunities arise.

At age-appropriate levels, and usually via ICT and PSHE, pupils are taught to look after their own online safety. From year 6, pupils are taught in the PSHCE curriculum about recognising safeguarding threats online, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL or any member of staff at the School.

From year 3, pupils are also taught about relevant laws applicable to using the internet. Pupils are taught about respecting other people's information and images etc. through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the School's Anti-bullying Policy). Pupils should approach the class teacher as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Use of school and personal devices

We have a real time monitoring system (ESafe) on all school pcs and laptops that will flag up to the Head and DSL any usage that is a cause for concern.

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff must ensure that it is locked to prevent unauthorised access.

Staff at the School are permitted to bring in personal devices for their own use. Staff are not allowed to have their phone switched on during the working day, unless they are in the School staffroom.

Personal telephone numbers may not be shared with pupils and under no circumstances may staff contact a pupil using a personal telephone number.

Pupils

Mobile technologies available for pupil use including laptops, tablets, cameras, etc. are stored in locked cupboards. Access is available via teachers or the IT technician and/or Network Manager.

No personal devices belonging to pupils are to be used during lessons at school with the exception of approved tablets under our Bring Your Own Device scheme (BYOD). Senior pupils may bring in mobile phones e.g. for safety purposes if they walk to and from school alone. They must be handed in to the Head of Seniors at the start of the day and collected as they leave school. Pupils should be aware that all IT use, including email communications can be monitored. This e-Safety policy and the AUP apply to all pupil and staff personal devices in school.

Use of internet and email

Staff

Staff must not access social networking sites, personal emails, any website or personal email which is unconnected with school work or business from school devices or whilst teaching in front of pupils. Such access may only be made from personal devices whilst in the staff room. When accessed from personal devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position.

There is strong anti-virus and firewall protection on the School network and, as such, it may be regarded as safe and secure. Staff should be aware that all IT use, including email communications can be monitored.

Staff must immediately report to the DSL or Head, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring the School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, sexting, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links or material which is discriminatory or offensive.

Under no circumstances must school pupils or parents be added as social network 'friends'. Any digital communication between staff and pupils or parents, carers must be professional in tone and content. Under no circumstances may staff contact a pupil, parent, carer from any personal email address. The School ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils from Year 3 are issued with their own personal VLe e-mail addresses. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work assignments / research / projects. Pupils should be aware that email communications are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails, certain websites and certain attachments should be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact their teacher. Staff must report such problems to the ICT technician and/or Network Manager.

Pupils should immediately report, to any member of staff, the receipt of any communication that makes them feel uncomfortable is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Pupils must report any accidental access to materials of a violent or sexual nature directly to any member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the School's Behaviour Management Policy. Pupils should be aware that all internet usage via the School's systems and its Wi-Fi network is monitored.

Data storage

The School takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the AUP for further details.

Staff and pupils are expected to save all data relating to their work to their school laptop or to the School's central server.

No personal data of staff, parents or pupils is to be stored on personal memory sticks. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the DSL.

Password security

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every 6 months;
- not write passwords down; and
- not share passwords with other pupils or staff.

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents, carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff must inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they must recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the AUP (concerning the sharing, distribution and publication of those images. Those images must only be taken on school equipment: personal equipment must not be used for such purposes or for storing these images.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.

Pupils must not take, use, share, publish or distribute images of others without their permission.

The Terms and Conditions of Admission state that we will include some photographs or images of pupils in the School's promotional material such as the prospectus, magazine, newsletter and website. Parents who do not want their child's photograph or image to appear in any of the School's promotional material must make sure their child knows this and must write immediately to the Head, requesting an acknowledgement of their letter. Photographs that include pupils, published on the School website, or displayed elsewhere, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Complaints

As with all issues of safety at school, if a member of staff, a pupil or a parent / carer has a complaint or concern please follow the complaints procedure available from the website or from the School office.

Any e-safety issues linked to Child Protection are to be dealt with using our Child Protection procedures.

Points of Reference

The Department of Education

The Independent Schools Inspectorate (ISI)

The South West Grid for Learning's template e-safety policies

The Office for Standards in Education (OFSTED)

http://www.childnet-int.org/

Related Policies

- Anti-Bullying Policy
- Child Protection and Safeguarding Policy and Procedures
- Staff Code of Conduct

LJB Nov 2016

Appendix – Acceptable Use Procedures

St. Aubyn's Pupil ICT 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 and communications 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 or devices under our 'Bring Your Own Device' (BYOD) scheme.

These procedures are intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications 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 ICT equipment (e.g. computers, cameras, phones, printers etc.).

ICT Equipment

- School IT systems are intended for educational use; pupils should not use the systems for personal or recreational use.
- 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 ICT equipment responsibly.
- Do not eat or drink in a computer room or near any ICT equipment.
- Only use ICT equipment for school work and homework.
- Do not print out homework on school printers.
- 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 ICT 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 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.
- Do not use external email, messaging or social networking sites or contact people unless as part of a school-approved scheme. Internal email through the VLe is acceptable.
- 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 I 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 ICT staff will be able to monitor individual use of ICT systems, including internet sites visited and use of the VLe; e.g. messages sent. Misuse of ICT 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 ICT equipment. Parents are expected to monitor carefully their children's use of ICT equipment and to support these rules outside of school.

M. Shute Nov 2016

St. Aubyn's Staff ICT Acceptable Use Procedures

The following procedures are designed to clarify to staff at St. Aubyn's what practices are acceptable when using digital technologies in and out of school: i.e. **email, Internet, intranet and network resources,** VLe, software, **equipment and systems.**

Staff must:

- only use the School's digital technology resources and systems for professional purposes or for personal uses deemed 'reasonable' (such as banking, shopping, emailing) by the Head and Governing Body when done in their own time.
- not reveal their password(s) to anyone.
- not allow unauthorised individuals to access school email / Internet / intranet / network, or other school systems.
- ensure that all documents, data etc., are saved, accessed and deleted appropriately.
- not engage in any online activity that may compromise their professional responsibilities.
- only use the approved, secure school email system for any school business.
- only use the approved school email, school VLe or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- not browse, download or send material that could be considered offensive to colleagues.
- report any accidental access to, or receipt of inappropriate materials, or filtering breach to their line manager and the Deputy Head.
- not download any software or resources from the Internet that are not adequately licensed or can compromise the network.
- not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and keep any 'loaned' equipment up-to-date, using the School's recommended anti-virus, firewall and other ICT 'defence' systems. Concerns or doubts must be passed to the ICT technician and/or Network Manager.
- not use personal digital cameras or camera phones for taking and transferring images of pupils or staff and they must not store images on personal equipment at home without permission.
- accept that any computer or laptop loaned to them by the School, is provided solely to support their professional responsibilities, is not for personal use and must be looked after.
- ensure that school equipment containing confidential data (e.g. parent contact information) is not taken away from school, unless it is password protected.
- understand that any information seen by them with regard to staff or pupil information, held within the School's information management system, will be kept private and confidential, except when it is deemed necessary that they are required by law to disclose such information to an appropriate authority.
- understand that all internet usage / and network usage can be logged and this information could be made available to line managers on request.

ICT work is the property of the School

Social Networking

Staff must:

- ensure that any private social networking sites / blogs etc. that they create or actively contribute to do not compromise their professional role.
- not view or update social networking sites (for personal use) during working times or on school equipment.
- not accept parents or pupils as friends on social networking sites.
- not discuss the School, colleagues, parents or pupils on social networking sites
- not post anything onto social networking sites that could offend any other staff member, parent of, or pupil at the School
- not post anything onto social networking sites that could be construed to have any adverse impact on the reputation of the School

M. Shute Nov 2016