Pupil ICT Acceptable Use Policy

Related to:

St James Senior Boys' School

Revision

All Statutory Policies are reviewed every year by members of the Senior Management Team at the School and approved by Governors on a regulated cycle. Any changes in legislation or specific procedures will be reflected in the policy as and when necessary and staff, parents and pupils will be informed of the changes (where appropriate).

Version Number:	1.3
Working Date:	11/06/2016
Legal Sign off by: **Date:**	Veale Wasbrough Vizards 27/04/2016
Type of Policy:	Regulatory
Authorised by:	
Effective date of Policy:	01/11/2016
Circulation:	Governors', SMT, Staff, Parents, Pupils
Status:	Final Draft

1 Policy Statement

1.1 Background

The School recognises that Information and Communication Technology (ICT) and the internet are fantastic tools for learning and communication which can be used in School to enhance the curriculum, challenge pupils, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the School community, but it is important that the use of the internet and ICT is seen as a responsibility and that pupils and staff use it appropriately. This policy gives guidance as to what is acceptable or not acceptable use of St James Senior Boys' school ICT systems and facilities.

2 Scope

2.1 This policy is available to parents on the School website and sent as a hard copy to all parents and pupils. The policy takes into account Keeping Children Safe in Education (2016), Working Together to Safeguard Children (2015), Mental Health and Behaviour in Schools (2016) Behaviour and Discipline in Schools (2016) and Preventing and Tackling Bullying (2014) by the Department for Education. Further guidance was sought from the UK Safer Internet Centre (www.safeinternet.org.uk) and CEOPS's Thinkuknow (www.thinkuknow.co.uk). The policy relates to the use of technology, including but not restricted to:

- E-mail
- The Internet
- Virtual Learning Environments in use at the School e.g. Firefly
- Social networking or interactive websites e.g. Facebook and Snapchat
- Instant messaging, chat room, blogs and message boards
- Games and gaming sites
- Mobile devices, tablets and iPads (including mobile phone and related applications) and mobile devices with the capacity for recording and/or storing still or moving images
- Webcams, video hosting sites e.g. YouTube
- Personal music players e.g. iPods
- Handheld game consoles
- Photographic or electronic equipment
- Wearable Technology e.g. Apple Iwatch

This policy applies to the use of any of the above on School premises and also any use, whether on or off School premises, 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.

Staff are subject to a separate policy which forms part of their Contract of Employment; further details can be found in the Staff Employment Manual. Staff receive regular safeguarding training which includes e-safety. Their training will ensure that they know how to identify pupils at risk and, in accordance with *Keeping Children Safe in Education (2016),* know how to refer children for further help.

Useful resources for pupils and parents are included in Appendix 3.

2.2 This policy can be made available in large print or other accessible formats if required.

2.3 **Aims**

This policy aims to be an aid in regulating ICT activity in School, and provide a good understanding of appropriate ICT use that members of the School community can use as a reference for their conduct online, inside and outside of School hours when using School owned facilities (including software platforms directly linked to the School). The overall aims are :

2.3.1 To encourage pupils to make good use of the educational opportunities presented by access to the internet and other electronic communication;

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

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

2.3.2.2 the sharing of personal data, including images;

2.3.2.3 inappropriate online contact; and

2.3.2.4 cyberbullying and other forms of abuse.

2.3.3 To minimise the risk of harm to the assets and reputation of the School;

2.3.4 To help pupils take responsibility for their own e-safety (i.e. limiting the risks that children and young people are exposed to when using technology);

2.3.5 To help children to be critical of the things that they see online, to report anything that concerns them and to know how to do that;

2.3.6 To ensure that pupils use technology safely and securely and are aware of both external and peer to peer risks when using technology.

3 Definitions

3.1 **Cyber bullying** is the misuse of ICT, particularly mobile phones and the internet deliberately to upset someone else (see Cyber bullying: advice for Head teachers and Teachers (2014); Advice for Parents and Carers on Cyber bullying (2014), written by the Department of Education). See Appendix 4 for more information about cyberbullying.

3.2 **E-safety** means limiting the risks that children and young people are exposed to when using technology, so that all technologies are used safely and securely.

4 Protocols

4.1 Pupils should comply with the following (but not limited to) protocols:

4.1.1 e-mail and internet protocol (Appendix 1)

4.1.2 mobile phone and mobile devices protocol (Appendix 2)

4.1.3 cyberbullying (Appendix 3).

5 Sanctions

5.1 Where a pupil breaches one of more of the School's protocol, the Governors have authorised the Head to apply any sanction, which is appropriate and proportionate to the breach, in accordance with the School's Behaviour and Discipline Policy including, in the most serious cases, permanent exclusion. Other sanctions might include increased monitoring procedures and withdrawal of the right to access the School's internet and email facilities. Any action taken will depend on the seriousness of the offence.

5.2 Unacceptable use of electronic equipment or the discovery of inappropriate data or files could lead to confiscation in accordance with the protocols attached to this policy and the School's policy on Behaviour and Discipline.

6 Procedures

6.1 Pupils are responsible for their action, conduct and behaviour on the internet in the same way that they are responsible during classes or break times. Use of technology should be safe, responsible and in accordance with the law. Any misuse of technology will be dealt with under the School's Behaviour and Discipline Policy. Permanent exclusion is the likely consequence for any pupil found to be responsible for material on his own or another website that would be a serious breach of School rules in any other context. If a pupil witnesses misuse by another pupil, then they should talk to a teacher about it as soon as possible.

6.2 Pupils must not use their own or the School's technology to cause harm to others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-Bullying Policy. If a pupil thinks that they might have been bullied or if they think another person has been or is being bullied, then they should talk to a teacher about it as soon as possible. See Appendix 3 for more information about cyberbullying.

6.3 If there is a suggestion that a child is at risk of abuse, the matter will be dealt with under the School's Safeguarding and Child Protection Procedures. If a pupil is worried about something that they have seen on the internet or on any electronic device, including on another person's electronic device, they should talk to a teacher about it as soon as possible.

6.4 In a case where the pupil is considered to be vulnerable to radicalisation they will 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 of being drawn into terrorism.

7 E-Safety Education

7.1 The School teaches e-safety throughout the curriculum, linked to the PSHE programme, attention is paid to teaching pupils how to manage their behaviours so that they can reduce any risk posed by young people or adults who use social media and the internet to groom, bully or abuse. Pupils are taught:

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

7.1.2 to be critically aware of content they access online and are guided to verify the accuracy of information;

7.1.3 how to recognise suspicious, bullying or extremist behaviour;

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

7.1.5 the consequences of negative online behaviour; and

7.1.6 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.

7.2 The role of parents in ensuring that pupils understand how to stay safe online is crucial. The School expects parents to promote safe online practice and to:

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

7.2.2 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

7.2.3 encourage their child to speak to someone if they are being bullied or need support.

7.3 Parents are invited to an annual talk regarding the proper use of the internet and mobile phone technology by the School.

7.4 If parents have any concerns or require any information about online safety, they should contact the Designated Safeguarding Lead.

7.5 Useful resources for pupils and parents are set out in Appendix 3.

8 Roles and Responsibilities

8.1 E-safety is a whole School responsibility but key individuals have specific responsibilities. The Head has ultimate responsibility for e-safety issues within the School. In addition, the Head will ensure that the Governing Body is kept informed of any relevant e-safety issues. The Head will ensure that there is appropriate funding to support internet safety initiatives throughout the School for both the technical infrastructure and INSET training and that internet safety is promoted across the curriculum. The Head, Deputy Head and Designated Safeguarding Lead (DSL), will ensure that the School continually filters the content of the internet sites accessed within the School and ensure that filtering methods are appropriate, effective and reasonable.

8.2 The Designated Safeguarding Lead will attend professional training on the safety issues relating to the use of the internet and other related technologies. He/ she will ensure that systems and procedures for supporting and/or referring pupils as a result of breaches of internet security are in place and are followed in any such cases. The school has a team that reviews and advises on e-safety policies, practices and procedures. This team will consist of the Deputy Head and DSL. The Deputy Head will develop management protocols so that any incidents in which internet safety are breached are responded to in an appropriate and consistent manner. He/she will liaise with the DSL to create an on-going staff development programme. This may include written information on internet safety, presentations at staff meetings and INSET days including hands-on training sessions on practical aspects of internet safety. The DSL liaises with the Heads of Year regarding issues about child protection. Internet safety issues are discussed at Senior Management level when or if they occur to ensure pupil safety.

8.3 The Governing Body has responsibility for child protection and health and safety, and elements of these will include internet safety. They will be kept informed of e-safety policy and ensure that appropriate funding is authorised for internet safety training and other activities as recommended by the Head.

8.4 The DSL – who has received training from the Child Exploitation and Online Protection (CEOP) – has a significant role to play in establishing and maintaining a safe ICT learning environment for the School. He/she will regularly liaise with the Head, Deputy Heads and any other relevant staff to ensure that educational and technological aspects of internet safety support and complement one another. In consultation with the Deputy Head, he/she ensures the appropriate and effective electronic security systems are in place, such as filtering, monitoring and firewall technology, virus protection supported further by regular and thorough monitoring of the computer networks in use at the School. He/she will ensure that the location of all internet-accessible computers within the School is documented so that in the event if a serious breach of internet safety, detailed, up-to-date documentation of the breach is available as evidence if required. He/she will make regular checks for indications of misuse are carried out and that any abuse is reported according to the correct procedure. He/she will also ensure that any illegal or indecent material found on the School network is reported.

9 The Liability of the School

Unless negligent under the terms of this policy the School accepts no responsibility to the pupil or parents caused by or arising out of a pupil's use of a mobile phone, wearable technology, email or the internet whilst at School.

9.1 The School does not guarantee to provide continuous internet access. Email and website addresses at the School may change from time to time at the discretion of the School.

9.2 For issues concerning the management of personal data please see the School's Data Protection Policy

10 Monitoring and Review

10.1 All serious ICT safety incidents will be logged in the e-safety electronic register.

10.2 The Designated Safeguarding Lead has responsibility for the implementation and review of this policy and will consider the record of ICT safety incidents and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and ICT safety practices within the School are adequate.

10.3 Consideration of the efficiency of the School's e-safety procedures and the education of pupils about keeping safe online will be included in the Governors' annual review of safeguarding.

Authorised by:	Chairman/Deputy Chairman of the Board of Governors Signature……..
Date:	November 2016
Circulation	[Governors / teaching staff / all staff / parents / pupils]

Appendix 1

Email and internet protocol (for pupils)

Introduction

1 We want you to enjoy using the internet, and to become proficient in drawing upon it during your time at the School, and as a foundation for your further education and career.

2 There are however some potential drawbacks with e-mail and the internet, both for you and for the School.

3 The purpose of this protocol is to set out the principles which you must bear in mind at all times and also the rules which you must follow in order for all pupils to use technology safely and securely.

Principles

4 For your own protection and that of others, your use of e-mail and of the Internet will be monitored by the School. Remember that when you delete an e-mail or file, this can still be traced and recovered on the School's IT systems and the IT systems of other providers that the School commissions to provide ICT services to you. Do not assume that files stored on servers or storage media are always private.

5 Passwords are there to protect the users of the School's systems. It is a serious offence to use the username and password of another pupil or staff member (users). Users should not reveal their password to any other user. A user whose account has been disabled by an Administrator must apply to an Administrator to have the account enabled at times when it is needed for lessons. This can be done via a member of staff or going to the IT Support Office. Impersonation of another user via e-mail is a serious offence. All of your files should be saved to your own area on the School network unless directed by a member of staff to the contrary

6 The use of e-mail and access to the internet from the School's computers or from a personal device and network must be for educational purposes only. You must not use the facilities for personal, social or non-educational use without the express, prior consent of a member of staff.

7 You must do all that you can to protect the security of the School's computer network and the security of networks belonging to others. In particular, this means being aware of the possibility of computer viruses and taking sensible precautions to avoid bringing them onto the School systems or passing them on to others. You should tell a member of staff if there is a failure in a technical safeguard e.g. if you gain access to a website you would expect to be blocked due to its content or if an area which should be password protected is not.

8 You must also try to protect personal and confidential information about yourself and others, even if you receive or come across this inadvertently. Receiving or using this kind of information may be unlawful under data protection legislation and laws relating to confidentiality.

9 You must not knowingly obtain (or attempt to obtain) unauthorised access to any part of any computer system, or any information contained on such a system. This is known as "hacking" and is both a criminal offence and a serious breach of School discipline.

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

11 You must not create, display, download, copy or otherwise distribute offensive material. Offensive material includes, but is not limited, to racism, sexism, pornography, bullying (including lesbian, gay, bisexual and transgender, LGBT bullying, defamation, and blasphemy, material which promotes radicalisation and extremism or criminal activity including hacking). In case of doubt, please ask a member of staff in the first instance. As far as you are able, you must make sure that you do not search for or receive such material. If you do come across such material, it is your responsibility to reject it and inform a member of staff immediately. Do not store executable files (.exe files) or other copyright material such as MP3 files, wallpapers, movie or movie clips and other formats in your user area other than those permitted for your studies.

12 You must not bring the School into disrepute through your use of e-mail, mobile devices or your access to the internet. For example, you must not send or ask to receive anything which you believe the Head/or your parents would find inappropriate for a pupil at St James Senior Boys' School.

13 You must not enter into any contractual commitment, whether for yourself or on behalf of another (including the School) without the advance written authority of the Head.

14 You will be liable to disciplinary sanctions including, in the most serious cases, permanent exclusion if you breach this protocol. The measures taken will depend on the seriousness of the offence. Normally a verbal warning will be issued for a minor misdemeanour but further sanctions may be taken against those who repeatedly offend or where the nature of the offence is more serious. You (or your parents) may also be asked to pay for any significant expenditure, or indemnify any significant liability incurred by the School as a result of the breach.

15 It is a serious offence to destroy work (files) of another user, or to create or introduce a virus or other malicious code (malware) to cause a system malfunction. This includes a denial of service (DOS) attack. Users must not attempt to reconfigure a computer, place shortcuts, aliases, install software or clip-art onto any local hard disk. Program files must not be downloaded from the internet. USB drives and CD-ROMs containing application software must not be brought into School. However, pupils may bring in work on USB drives, if approved by staff beforehand. Pupils should select to scan the USB drive before accessing files.

16 You should treat all ICT facilities responsibly, and avoid waste by not sending documents to print unless you have first previewed them, and are sure they are in final draft form. Colour printing is permitted, but pupils are expected to use the printing facility sparingly and to not print off web pages unless absolutely necessary.

17 Pupils are not allowed to access interactive or networking web sites or applications when using School computers or, if using personal laptops or other devices, on School premises.

Rules

18 You may only use the School's computers whilst logging on with your own username and password.

19 You must never disclose your password to another pupil, nor to anyone outside of the School.

20 You may not read anyone else's e-mails.

21 You must not send an email to an entire address list or distribution list without the express, prior consent of a member of staff.

22 You must not use the School's computer system to play non-educational games, or use "chat" programmes, bulletin boards, user groups etc. unless directed to do so by a member of staff.

23 You must not use personal web-based e-mail accounts such as Yahoo, Hotmail or Gmail. This will be unnecessary as you are provided with your own personal e-mail account by the School.

24 Pupils must use their School email accounts for any email communication with staff. Communication either from a pupil's personal email account or to a member of staff's personal email account is not permitted.

25 You may not send or receive e-mail messages, attachments or program files greater than five megabytes in size.

26 You must tell a member of staff immediately if you have accidentally read, downloaded or have sent inappropriate material, including personal information about someone else.

27 If you think or suspect that an attachment sent to you, or other material which you want to download, might contain a virus, you must not open the attachment or download the material without first speaking to a member of staff or ICT Support to arrange a virus check.

28 You must not cancel or remove the School auto signature/disclaimer attached to all e-mail messages.

29 You must not send or receive encrypted messages.

Appendix 2

Mobile electronic devices protocol (for pupils).

1. "Mobile electronic device" includes without limitation mobile phones, iPads, Tablets, Laptops, MP3 players or other wearable technology.

2. The use of mobile electronic devices is not allowed at any time on School premises without the permission of a member of staff. Phones and other mobiles must be kept switched off at all times unless being used for an educational purpose with the specific permission of a member of staff. Improper use of phones and other mobile electronic devices will result in a Red Card and the device will be confiscated for the rest of that day. A repeat offence will result in a prolonged confiscation and then a permanent ban.

3. In emergencies, pupils may request to use the School telephone. Parents wishing to contact their children in an emergency should always telephone the School Reception and a message will be relayed promptly.

4. Pupils may not bring mobile electronic devices into examination rooms under any circumstances, except where special arrangements for the use of a tablet or laptop have been agreed with the School in writing. Such an offence will result in immediate disqualification.

5. 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 the pupil is 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 and Discipline Policy) and the School's safeguarding procedures will be followed in appropriate circumstances (see the School's Safeguarding and Child Protection Policy and procedures).

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

7. The School reserves the right to confiscate a pupil's mobile electronic device including wearable technology for a specified period of time if the pupil is found to be in breach of this protocol. The pupil may also be prevented from bringing a device to the School temporarily or permanently and at the sole discretion of the Head.

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. Pupils are not allowed to operate a device with the capability of recording and/or storing still or moving images on School premises except with the express permission of the member of staff in charge and the permission of all those appearing in the image (still or moving).

3. All pupils must allow staff access to images stored on any device that has been brought onto School premises and must delete images if requested to do so.

4. Posting of photographic material which, in the reasonable opinion of the Head, is considered to be offensive on websites such as YouTube, Facebook etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material or when the submission

occurred. This is the position whether the device used is a School computer or a mobile electronic device or computer operated elsewhere including the pupil's home.

5. Pupils are reminded that 'sexting' (sending or posting messages,images or videos of a sexual or indecent nature) is strictly prohibited by the School and may constitute a criminal offence. The School will treat incidences of sexting (both sending and receiving) as a safeguarding matter under the School's child protection procedures (see the School's Safeguarding and Child Protection Policy and procedures). Pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

6. Mobile electronic devices may be confiscated and searched in appropriate circumstances. If the Head has reasonable grounds to believe that a pupil's mobile device, camera or personal laptop contains images, text messages (SMS) or other material that may constitute evidence of criminal activity, he / she may hand the device to the police for examination.

7. Use of cameras, mobile devices with camera facilities or laptop computers in breach of this protocol may result in confiscation of the equipment until the end of term and the pupil may be permanently banned from bringing a camera, mobile device or laptop onto School premises in the future.

Appendix 3

Cyberbullying

Cyberbullying is the misuse of ICT, particularly mobile phones and the internet to deliberately upset someone else.

Pupils should remember the following:

Always respect others - be careful what you say online and what images you send.

Think before you send - whatever you send can be made public very quickly and could stay online forever.

If you are or someone you know is being cyberbullied, TELL SOMEONE. You have the right not to be harassed or bullied online. Tell an adult you trust - your parents, any member of staff, or a helpline such as ChildLine on 0800 1111. See the School's Anti-Bullying Policy for further guidance.

Don't retaliate or reply online.

Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the School to investigate the matter.

Block the bully. Most social media websites and online or mobile services allow you to block someone who is behaving badly.

Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

Any incident of cyberbullying will be dealt with in accordance with the School's anti-bullying policy and, where applicable, the behaviour and discipline policy.

Useful resources for pupils and parents
http://www.saferinternet.org.uk/
http://www.kidsmart.org.uk/
http://www.safetynetkids.org.uk/
http://www.safekids.com/
http://www.thinkuknow.co.uk/
DfE's Advice for Parents and Carers on Cyberbullying
http://parentinfo.org/
DfE's Advice on the use of social media for online radicalisation

The Surrey Safeguarding Children Board has produced guidance for parents on radicalisation which is available here: https://www.surreycc.gov.uk/people-and-community/family-information-service/support-and-advice-for-parents-and-carers/keeping-your-family-safe/radicalisation

Annex

Pupil/School Contract for Use of the Computers – Signatures

Pupil
Write in your name clearly below, then sign and date underneath:

I, ……....., in Form……., have read and understood the Pupil ICT Acceptable Use Policy and will endeavour to follow the rules conscientiously and to the best of my ability. I understand that if I break any of these rules, I may forfeit my opportunity to use some or all of the computing facilities at the School and may also face other punishment as for any of the School rules.

Pupil's Signature …… Date:……/……/ ……

Parent
Write in your name clearly below, then sign and date underneath:

I, ……....., have read and understood the Pupil ICT Acceptable Use Policy and agree for my child to use computer facilities at School bound by these rules. I will support my child in following these rules and understand that he may forfeit his opportunity to use some or all of the computing facilities if he breaks them.

Parent's Signature …… Date:……/……/ ……