Acceptable Use Policy (Whole School including EYFS)

Independent Day School for Boys and Girls

Our Lady of Sion School

Reviewed: 13 October 2019

Frequency of review: 3 years

Next review: October 2022

1 Scope

1.1 This policy has been authorised by the Governors and is addressed to all pupils. It is available to parents on request and parents are encouraged to read it. This policy relates to the use of technology, including:

- the internet
- e-mail
- Virtual Learning Environments such as Firefly
- social networking or interactive web sites
- instant messaging, chat rooms, blogs and message boards
- gaming sites
- mobile phones and smartphones
- tablets
- devices with the capability for recording and / or storing still or moving images
- webcams, video hosting sites (such as YouTube)
- personal music players such as iPods
- handheld game consoles
- SMART boards
- other photographic or electronic equipment.

1.2 It 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 where the culture or reputation of the School are put at risk.

2 Aims

2.1 The aims of this policy are:

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

2.1.2 to safeguard and promote the welfare of pupils by preventing "cyberbullying" and other forms of abuse;

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

2.1.4 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); and

2.1.5 to ensure that pupils use technology safely and securely.

3 Internet and e-mail

3.1 The School provides internet access and an email system to support its academic activities.

3.2 If, at any time after that, you are unsure whether you are doing the right thing, you must ask for help from a member of staff, whilst using email or the internet

3.3 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 even when you have deleted an e-mail or something you have downloaded, it can still be traced on the system. Do not assume that files stored on servers or storage media are always private.

3.4 Protocols

3.4.1 Pupils should comply with the following protocols as well as complying with the rules about security set out in section 4 below:

(a) internet protocol (Appendix 1);

(b) e-mail protocol (Appendix 2);

(c) protocol for communication between staff and pupils (Appendix 3).

3.4.2 Please also see the School's separate E-Safety Policy.

4 Security

4.1 Pupils who are concerned about any aspect of the safety and security of the School's networks should speak to Network Systems Manager or Deputy Headmaster/Senior Teacher (JS).

4.2 The School has a firewall in place to ensure the safety and security of the School's networks and additional devices may be installed in the future to further protect these networks. Pupils must not attempt to disable, defeat or circumvent any of the School's security facilities.

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

4.4 Passwords

4.4.1 All pupils have an ID and passwords to log onto the School's network and password protected screensavers are used on all workstations. Passwords protect the School's network and computer system and the following rules apply:

(a) ID and passwords should be kept confidential and passwords must be changed immediately if it is believed someone else knows it;

(b) pupils must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which he / she is not authorised access;

(c) pupils should log off if leaving workstations for any period of time.

4.4.2 It is a serious offence to use the user ID and password of another user.

4.5 Anti-virus

4.5.1 Anti-virus software is installed on every PC connected to the School's network. Pupils must ensure this is running at all times and report any problems to the IT department immediately. Users of the School's facilities should be aware of the potential damage that can be caused by computer viruses and the following rules apply:

(a) anti-virus software must not be disabled or uninstalled for any reason;

(b) any pupil believing he / she has received a message that includes a virus must not open it and report it to the Network Systems Manager or Deputy Headmaster immediately;

4.5.2 It is common for a virus to be circulated as an e-mail attachment and to use an email account address book to forward itself to others. This means an infected email could be received from a known and trusted source. If the email looks unusual, pupils should be suspicious and if there is any doubt as to the authenticity of an email, it should be reported to the Network Systems Manager or Deputy Headmaster immediately.

5 Procedures

5.1 Pupils are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible and legal. Pupils witnessing misuse by other pupils should talk to a member of staff about it as soon as possible.

5.2 Any misuse of the internet will be dealt with under the School's Behaviour and Discipline Policy.

5.3 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 Procedures. See also the School's E-Safety Policy. If you think that you might have been bullied or if you think another person is being bullied, talk to a member of staff about it as soon as possible.

5.4 If there is a suggestion that a child is at risk of significant harm, the School's Safeguarding procedures will be followed. Pupils who are worried about something that they have seen on the internet should talk to a member of staff about it as soon as possible.

6 Sanctions

6.1 Where a pupil breaches any of the School's protocols, the Governors have authorised the Headmaster to apply any sanction which is appropriate and proportionate to the breach including, in the most serious cases, expulsion. Other sanctions might include: increased monitoring procedures, detention, withdrawal of privileges and suspension.

6.2 Expulsion is the likely consequence for any pupil found to be responsible for electronic material on his or her own or another device that would be a serious breach of School rules in any other context.

6.3 Unacceptable use of electronic equipment could lead to confiscation in accordance with the protocols attached to this policy and the School's policy on Behaviour and Discipline, including the policy on the searching and confiscation of electronic devices.

6.4 The School reserves the right to charge the pupil or his / her parents for any expenditure incurred by the School as a result of a breach of this policy.

7 Monitoring and review

7.1 All serious e-safety incidents will be logged in the E-Safety log.

7.2 The Deputy Headmaster *(together with Senior Teacher (JS)/Assistant Head (Pastoral), who will feed in on E-Safety)* has a responsibility for the implementation and annual review of this policy, in consultation with parents, pupils and staff. The Deputy Headmaster will consider the record of e-safety incidents and new technologies. The Deputy Headmaster will consider if existing security procedures are adequate.

7.3 The Deputy Headmaster will make an annual report to the governors on the effectiveness of the School's Acceptable Use Policy.

Authorised by SLT

Date 13/10/19

Related documents:
Safeguarding policy
Behaviour & Discipline Policy
Disciplinary Policy
Anti-bullying Policy
E-Safety Policy (formerly E-Safety Policy)
E-Safety Log

Appendix 1 Internet protocol

1 Introduction

1.1 We want each pupil to enjoy using the internet, and to become proficient in drawing upon it both during your time at School, and as a foundation for your further education and career. However, there are some potential drawbacks with the internet, both for you and for the School.

1.2 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.

1.3 The rules set out below will also apply to the use of e-mail in as much as they are relevant.

2 Use of the internet

2.1 During School hours you must use the internet for educational purposes only to research relevant topics and obtain useful information. Access to the internet is available in the Senior School Library, Lower & Upper IT Suites as well as via a wireless network. Internet is also available in the Junior School ICT Suite.

2.2 Only at the following times may pupils access the internet at School for personal activities including communication and recreational use:

(a) Before the start of the school day, during break times and after school subject to the other conditions within this Acceptable Use of ICT Policy and the E-Safety Policy.

2.3 You must not create, display, copy or otherwise distribute offensive material. Offensive material includes but is not limited to racism, sexism, pornography, bullying (including homophobic bullying), defamation, blasphemy or criminal activity including hacking and radicalisation. In cases of doubt, please ask any member of staff. As far as you are able, you must also make sure that you do not search for or receive such material. It is your responsibility to reject it if you come across it, and to inform a member of staff.

2.4 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.

2.5 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.

2.6 Do not store executable files (.exe. files) or other copyright material such as MP3 files, wallpapers, movie clips and other formats or movie clips in your user area.

2.7 You must not bring the School into disrepute through your access to the internet. For example, you must not send or ask to receive anything which you believe the Headmaster or your parents would find inappropriate for a pupil at the School.

2.8 You must not enter into any contractual commitment, whether for yourself or on behalf of another (including the School).

2.9 Users must not attempt to reconfigure the computer, place shortcuts, aliases, software or Clip Art onto any local hard disk. Programme files must not be downloaded from the internet. Personal USB pen drives and CD-ROMs containing application software must not be brought into School.

2.10 You should treat all ICT resources 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 this facility sparingly and not print off web pages unless absolutely necessary. All printing is monitored.

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

2.12 You must not use the School's computer system to play non-educational games, or use "chat" programmes, bulletin boards, user groups etc.

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

Appendix 2 Email protocol

1 Introduction

1.1 We want each pupil to enjoy using e-mail, and to become proficient in drawing upon it both during your time at School, and as a foundation for your further education and career. However, there are some potential drawbacks with the use of e-mail, both for you and for the School.

1.2 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.

1.3 The School has systems in place that monitor and record all e-mail usage. The School reserves the right to remove the e-mail facility from any pupil who does not observe this policy.

2 Use of email

2.1 E-mails sent from pupils' School email accounts will be taken as representing the School and the same standards of courtesy must be applied as in the case of any other form of communication undertaken on behalf of the School. Pupils should think carefully about what is said about individuals and organisations when sending e-mails.

2.2 E-mail must be used for educational purposes only during School hours.

2.3 You must not use web based e-mail accounts such as Yahoo, Hotmail or USA.NET. This will be unnecessary as you are provided with your own personal e-mail account. You can access your School e-mail from home by going to https://mail.sionschool.org.uk then enter your username in the space provided. (the password field is your normal logon password).

2.4 You may send and receive e-mail and have access to the internet at School only during term time and only during the School day. (The School will not forward e-mails received during the School holidays.)

2.5 Appropriate authority must be obtained to send an e-mail anywhere outside of the School community.

2.6 Pupils must not read anyone else's e-mails without their consent.

2.7 Pupils must consider carefully whether to give out their external e-mail address. E-mail circulation lists operate in the same way as junk mail; continuity of service can be seriously affected by unsolicited messages, some of which may contain malicious code or virus.

2.8 Pupils should avoid sending large graphics and scanned images and must not send or receive e-mail messages, attachments or program files greater than 20 megabytes.

2.9 Pupils are responsible for their own e-mail housekeeping. Unwanted e-mails should be deleted and those to be retained should be archived regularly.

2.10 E-mailing your home e-mail address is permitted; for example to e-mail documents home to work on, then e-mailing them back to School thereafter.

3 Misuse

3.1 Abuse or misuse of the e-mail system will be subject to disciplinary action in accordance with Our Lady of Sion's disciplinary policy. Examples include e-mails that could be considered to be:

(a) indecent, obscene, pornographic or illegal

(b) offensive or abusive, a personal attack, rude or personally critical, discriminatory, or generally distasteful to encourage or promote activities which make unproductive use of School time

(c) involving activities outside the scope of pupils' responsibilities; for example, unauthorised selling/advertising of goods or services

(d) affecting or having the potential to affect the performance of, damage or overload the School's systems, network and/or external communications in any way

(e) in breach of copyright or licence provision with respect to both programmes and data

(f) impersonation of another user.

3.2 You must not bring the School into disrepute through your access to the internet or e-mail. For example, you must not send or ask to receive anything which you believe the Headmaster or your parents would find inappropriate for a pupil at the School.

3.3 Any use of e-mail that is not in accordance with this policy will be dealt with as a disciplinary matter.

Appendix 3 Protocol for communication between staff and pupils

1 Mobile phones

1.1 Our Lady of Sion School is committed to safeguarding and promoting the welfare of children at the School. As part of our safeguarding policy we expect staff and pupils, and where appropriate, parents, to follow this protocol on communication by mobile phone. Throughout this protocol the term mobile phone includes a PDA or similar device. See also the separate E-Safety Policy for the School's general policy on the use of mobile electronic devices in School.

2 On school premises

2.1 Staff and pupils should avoid using mobile phones to speak to or send each other messages whilst in School. Telephone numbers should not be exchanged or displayed. Any messages that are sent should be brief and courteous.

3 Emergencies

3.1 Staff on supervisory duties in the playground, on playing fields or in relation to transport may carry and use a mobile phone to seek assistance from colleagues or emergency services.

3.2 Where a pupil or group of pupils are involved in an emergency situation they may use a mobile phone to seek assistance.

4 Outside school

4.1 Again, staff and pupils should avoid using mobile phones to speak to or send each other messages outside School. Any messages that are sent should be brief and courteous.

4.2 The leader of an educational visit may carry a mobile phone supplied by the School and, as part of the preparations for the visit, will ensure that other adults taking part in the visit are equipped with mobile phones and that relevant numbers are exchanged, where possible.

4.3 Staff and pupils taking part in such visits should avoid using mobile phones to speak or send messages to each other except in emergencies. Any messages that are sent should be brief and courteous.

5 Inappropriate communications

5.1 If there are reasonable grounds to believe that inappropriate communications have taken place, the Headmaster will require the relevant mobile phones to be produced for examination. The usual disciplinary procedures will apply. Pupils may expect to have mobile phones confiscated if there has been a breach of this protocol.