The Skinners' School

Acceptable use of the Internet Policy

Policy Area:	Pastoral and Safeguarding
Reviewed:	June 2018
Adopted:	June 2014
Next Review:	June 2019
Governing Committee:	Education Committee
LG Responsibility:	Julian Metcalf

The Skinners' School

Acceptable use of the Internet Policy

ICT and the related technologies such as the Internet and email are an important part of learning in The Skinners' School.   We expect all students to be responsible for their behaviour when using ICT and the Internet.

Permission to use the facilities is conditional upon the user agreeing to abide by the "Acceptable Use Policy", a copy of which is signed by students when they join The Skinners' School. Any breaches of this policy will be treated as a disciplinary matter and dealt with appropriately. Sanctions imposed could result in the right to use the facilities being withdrawn either temporarily or, under certain conditions, permanently.

This policy should be read in conjunction with the School Behaviour Policy and Safeguarding Policy which make specific reference to cyber-bullying and the sanctions associated with such misbehaviour.

Network

- Students will only access The Skinners' School computer network with their own user name and password. Students will follow The Skinners' School's ICT security procedures and not reveal their password to anyone.
- Students may be held responsible for any activity that takes place using their network account.
- Students must inform their teacher/ICT staff whenever a breach of security is suspected.
- Students will not access or attempt to access other people's files.
- Students will log off correctly and leave the equipment set up ready for the next person to use.
- Students will use the computers for schoolwork and homework only, unless directed to a site by a member of staff i.e. Yearbook, D of E etc.
- Students will not cause damage to, or interfere with, any of the ICT equipment.
- Students will handle all computer equipment carefully.
- Students will not use any media or connect any hardware (CDs, DVDs, USB-drives, MP3 players, cameras etc.) in their user area unless directed by a member of staff as part of their work.
- Students will not save any other type of file in their user area eg. .zip or .exe files etc.
- Students will report any unpleasant material, messages sent to them or misuse of computers. Students understand this report would be confidential and would help to protect other students and themselves.
- Students understand that any action that threatens The Skinners' School network (e.g. hacking) will not be tolerated under any circumstances. Any such misuse will be dealt with very severely.

Internet Use

- Students will not use the internet without the permission of the member of staff in charge of the room.
- Students will be responsible for their behaviour when using the Internet. This includes the resources they access and the language they use.
- Students will not deliberately browse, download or upload material that could be considered offensive or illegal. If students accidentally come across any such material they will report it immediately to their teacher.
- Students will not access public chat rooms, forums and social networking sites.
- Students will only use Skinners' School message boards, discussion forums and other electronic communication forums for educational purposes and these will always be supervised.
- Students will not copy information into assignments without acknowledging the source, because of plagiarism and copyright infringement.
- Students will not play multiplayer network games.

E-mail

- Students will not send any e-mails during lesson time without the permission of the member of staff in charge of the room.
- Students will only e-mail people they know, or people approved by their teacher.
- Students will only send attachments that are relevant to their school work.
- Students will not open e-mail attachments from people they do not know.
- Students will make sure that all ICT communications with any student, teacher or others are sensible.
- Students will not send material that could be considered offensive or illegal to any student, teacher or others.
- Students will not send anonymous messages or forward chain letters.
- Students will not send messages which appear to come from someone else.
- Students will not give out any personal information such as name, phone number or address. Students will not arrange to meet someone unless this is part of a school project approved by their teacher.
- Students will report any unpleasant material or unpleasant messages received via email.

Personal Devices

Students must be responsible and respectful about the use of their own technology within The Skinners' School. Leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera, still or moving ,is in direct breach of the Skinners' School's acceptable use policy. Although mobile phones are permitted at The Skinners' School, they must be turned off during the school day. They are not to be used in class under any circumstances, unless specific permission has been granted. Use of 'bluetooth' functions is prohibited.

Social Media

Students are encouraged to follow the guidelines set by social media organisations (eg Facebook, Twitter) if using these sites outside the school day. It is not permissible for students to access social media sites from school ICT devices. Students should act responsibly at all times when using social media websites and should report any issues of cyper-bullying immediately to a member of staff at The Skinners' School, their parents, and the appropriate website authorities. The school treats issues relating to e-safety and cyber-bullying very seriously and this is addressed in the School's Safeguarding Policy and in the definition of cyber-bullying given below. Students are also taught skills' relating to safe use of the internet in both PSHE and ICT lessons.

General

- Students should store copies of all important work in their "My Documents" for safe keeping as this area is backed up daily – this is for school work only.
- No music, video or program files should be stored in "My Documents" unless directed to do so by a member of staff.
- Students should understand that the Skinners' School will monitor the use of The Skinners' School network including email and the use of the Internet by students.
- Students should understand that The Skinners' School may check their computer files.
- Students should understand that copyright laws and intellectual property rights must be respected.

Please Note:

- The Skinners' School puts, as its top priority, the security of its network and the safety of its users. Action by any user that compromises these aims, in any way, will be dealt with very seriously as too will any action that adversely affects the smooth running of The Skinners' School network.
- The Skinners' School reserves the right to examine or delete any files that may be held on its computer system and to monitor any Internet sites visited.

- The Skinners' School reserves the right to randomly check the contents of any computer or storage media connected to The Skinners' School network. This includes flash drives, CDs, DVDs, MP3 players, I-pods, mobile phones or any other form of storage medium.
- Any unsuitable material will be deleted or destroyed and suitable disciplinary action taken.
- Any large non-academic files (e.g. mp3 or jpg files) will be deleted from the network after consultation with relevant staff.
- Any use of phones in connection to computers is not acceptable unless authorised by a member of staff.

Definitions

"Hacking" is defined as any action, malicious or otherwise, that is designed to gain unauthorised access to network, computer or user information or to harm or take control of any computer system.

"Inappropriate material" includes any material that is deemed to be dangerous, pornographic, offensive, racist, sexist, illegal and any other material deemed by the school to be inappropriate for students.

"Cyber bullying" is the use of ICT for bullying purposes: in order to combat cyber-bullying, The Skinners' School will use its designated power to regulate the conduct of students off-site when this is appropriate. Cyber-bullying does differ form other forms of bullying in that there is usually evidence left behind (in the form of emails, text messages, social media posts etc.) There are also a number of methods of reporting and restricting this form of bullying through alerting mobile phone companies and networking site operators. Normal school sanctions will apply, and may also result in restrictions placed on a student's use of ICT.

Sanctions

- Violations of these rules or any other action that is inappropriate or endangers The Skinners' School network may result in the withdrawal of access to the ICT resources.
- Additional action will be taken by The Skinners' School in line with existing practice regarding inappropriate behaviour and safeguarding.
- For serious violations, exclusion may be imposed.
- Where appropriate, police may be involved or other legal action taken.

June 2018