BEECHWOOD
Sacred Heart School

PUPIL COMPUTER, IPOD AND MOBILE TELEPHONE ACCEPTABLE USE POLICY (PUPILS)

Acceptable Use Policy
This policy relates to the use of technology, including:

- e-mail
- the internet
- social networking or interactive websites, for example Facebook, Twitter, MySpace, Ask FM, and Instagram.
- instant messaging, chat rooms, blogs and message boards
- gaming sites
- mobile phones (including PDA and similar devices)
- mobile phones with the capability for recording and/or storing still or moving images
- webcams, video hosting site (such as YouTube)
- personal music players such as iPods
- handheld game consoles
- SMART boards
- other photographic or electronic equipment.

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.

This policy can be made available in large print or other accessible format if required. Other policies and documents which should be read in conjunction with this policy are Keeping Children Safe in Education (September 2016), Prevent Duty (March 2015) The use of social media for online radicalisation (July 2015) Working together to safeguard children (March 2015), AUP for Educational Settings and their Wider Communities (KCC September 2016) and the school's Safeguarding Policy and Anti bullying Policy.

Definitions:

Cyber-bullying is the use of information and communication technology (ICT), particularly mobile phones and the internet deliberately to upset someone else.

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.

Introduction

The following document is divided into four sections as follows:

1. The SMART Rules.
2. The Quick Guide.
3. Full Draft Policy Document.
4. Guidelines and Good Advice

1. **SMART Rules**

S **Safe** - Keep safe by being careful not to give out personal information, such as your full name, email address, telephone number, home address, photos or School name, to people you have only had contact with online.

M **Meeting:** Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or guardians' permission and even then only when they can be present.

A **Accepting:** Accepting emails, instant messages, or opening files, pictures or texts from people you don't know or trust can lead to problems; they may contain viruses or nasty messages!

R **Reliable:** Information you find on the Internet may not be true, or someone online may be lying about who they are.

T **Tell:** Tell your parents, guardian or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at: www.thinkyouknow.co.uk and/or use the CEOPS icon on all school computers and you can report anything you are not happy about to anyone you feel you trust. This could be your tutor, Head of Division, Deputy Head, guardian, parent or someone else's parent. Tell someone. The Deputy Head, Mrs Rowe who is also the Designated Safeguarding Lead is also the E Safety lead.

2. The Quick Guide: Pupil Computer, Mobile and IPod Use

- You may only log on as yourself. Do not give your password to anyone else.
- Be aware that the School can check your computer files and which sites you visit at any time.
- Do not use bad language, bully or try to access inappropriate material on line.
- Personal I-Pods, mobile telephones and other electronic devices are subject to the guidance and rules already in place as found in the School's *Mobile Phone Policy*, and the *iPad Policy*.
- In lessons where computers are being used, internet browsers *may not* be switched on unless permission has been given by the teacher to use the internet.
- Similarly, under no circumstances are you to use social networking sites, email or Skype during lesson times. Facebook cannot be used during school time. The school's *Social Networking Sites Policy* sets out our reasons in more depth. Guidance and general safety advice regarding social networking sites is available at the end of this document.
- You are not to record anything during lessons unless the teacher requests that you do so using technology. On the rare occasion that you are given permission (or indeed if you have filmed/recorded material without permission) to record anything, the contents of that recording are not to be uploaded onto the web, e.g., Facebook or YouTube for any reason. **The School will view this as serious disciplinary matter**.
- You must not wear earphones when walking around the site at any time.
- Do not attempt to bypass school web filters.
- Do not give out your personal details online and never arrange to meet a stranger.
- Respect copyright and do not plagiarise (copy) work.

3. Pupil Computer Acceptable Use Policy

The use of the latest technology is actively encouraged at Beechwood Sacred Heart but with this comes a responsibility to protect pupils, staff and the School from abuse of the system.

All pupils, therefore, must adhere to the Policy set out below. This Policy covers all workstations, laptops, mobile telephones and electronic devices within the School, irrespective of who is the owner.

All pupils are expected to behave responsibly on the School computer network, as they would in classrooms and in other areas of the School.
Pupils with SEN or other disabilities may need extra support to understand the AUP document and to act safely on line.

1. Personal Safety

- Always be extremely cautious about revealing personal details and never reveal a home address, telephone number or email address to strangers.
- Do not send anyone your credit card details or anyone else's or any other details without checking with an adult first.
- Always inform your teacher or another adult if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way.
- Do not play with or remove any cables that are attached to a School computer.
- Always be yourself and do not pretend to be anyone or anything that you are not on the Internet.
- Never provide false information over the internet, e.g., a date of birth that makes you older than you are.
- Do not arrange to meet anyone you have met on the Internet; people are not always who they say they are.
- If in doubt, ask a teacher or another member of staff.
- Use the CEOPS icon on your computer for advice and to report any incident which concerns you.

2. System Security

- Do not attempt to go beyond your authorised access. This includes attempting to log on as another person, sending e-mails whilst masquerading as another person or accessing another person's files. Attempting to log on as staff is unacceptable and may result in the loss of access to systems and other serious sanctions. You are only permitted to log on as yourself.
- Do not give out your password to any other pupil; if you do and they do something wrong logged on as you, you will be held responsible. If you

suspect someone else knows your password, change it immediately by going to the ICT Department.

- Do not make deliberate attempts to disrupt the computer system or destroy data, e.g. by knowingly spreading a computer virus.

- Do not alter School hardware in any way.

- Pupils are encouraged to email Study to the School system. By doing so we minimise the risk of viruses entering the School's Network.

- Memory sticks can only be used on computers that have USB ports but should be kept to minimum. Again, you are encouraged to send work via email.

- Do not knowingly break or misuse headphones or any other external devices, e.g. printer or mouse.

- You may use your own headphones only if there is a headphone socket on the front of the workstation and only with permission.

- Do not attempt to connect to another pupil's laptop or device while at School. Establishment of your own computer network is not allowed.

- Do not take, eat or drink into the Computer Rooms.

- Do not play games by or near any computer equipment.

- Please leave the Computer Room tidy. Log off, check that you have left your station looking tidy.

3. Inappropriate Behaviour

'Inappropriate Behaviour' relates to any electronic communication whether email, blogging, tweeting, social networking, texting, journal entries or any other type of posting/uploading to the Internet.

- Do not use indecent, obscene, offensive or threatening language.

- Do not post or send information that could cause damage or disruption.

- Do not engage in personal, prejudicial or discriminatory attacks.

- Do not harass another person. 'Harassment' is persistently acting in a manner that distresses or annoys another person.

- Do not knowingly or recklessly send or post false, defamatory or malicious information about a person.

- Do not post or send private information about another person without their prior agreement.

- Do not use the Internet for gambling.

- Bullying of another person either by email, online or via texts will be treated with the highest severity. The School will enforce its sanctions to if this policy is breached outside of School, e.g., posting of offensive and hurtful images or comments about a pupil within Beechwood. **(See guidelines on Cyber Bullying below)**

- Do not produce or send sexual imagery. This is a form of abuse and is a safeguarding issue. The Designated Safeguarding lead will be informed and if necessary the Police and your parents will be contacted.

- Do not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people.

- If you mistakenly access such material, please inform your teacher or another member of staff immediately or you may be held responsible.

- If you are planning any activity which might risk breaking the Pupil Acceptable Use Policy (e.g. research into terrorism for a legitimate project), an appropriate member of staff must be informed beforehand.

- Do not attempt to use proxy sites (a site often pretending to be something it is not) on the Internet.

- Do not take or post a photo of another pupil or member of staff without their permission.

4. Email

- You should check your School email at least once a day during term time for new messages.

- Do not reply to spam mails as this will result in more spam. Delete them and inform the IT Department.

- Do not open an attachment from an unknown source. Inform IT as it might contain a virus.

- All emails sent from the School reflect on the School name so please maintain the highest standards.

- Do not use email (including web mail) during lessons unless your teacher has given permission.

- Do not send any files above 10mb by mail. Please ask IT if you require this temporarily to be lifted.

- Do not send or forward annoying or unnecessary messages to a large number of people, e.g. spam or chainmail.

- Do not join mailing lists without the prior permission of IT.

- Only send mail to a distribution list if you really have to.

- If you receive an email sent to you in error, please inform the sender as soon as possible.

5. Plagiarism and Copyright

- Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the Internet or anywhere else.

- You should respect copyright. Breaking copyright law occurs when you reproduce a piece of work. You should request permission from the copyright owner. This includes music files and the copying of CDs, downloading of films from illegal sites and other such formats.

6. Privacy

- All files and emails on the system are the property of the School. As such, system administrators and staff have the right to access them if required.

- Do not assume that any email sent on the Internet is secure.

- All network access, web browsing and mails on the School system are logged.

- If you are suspected of breaking this Policy, your own personal laptop/device and mobile telephone can be searched by staff with the permission of your parents.

- The School reserves the right to randomly search the Internet for inappropriate material posted by pupils and to act upon it.

7. Software

- Do not install any software on the School system.

- Do not attempt to download programs from the Internet onto School computers.

- Do not knowingly install spyware or any sort of hacking software or device.

8. Sanctions

- Sanctions will vary depending on the severity of the offence; they will range from a warning or withdrawal of Internet use, to suspension or expulsion.

- A breach of the law may lead to the involvement of the police if a pupil is looking at pornography or is generating or producing sexual imagery or is regularly accessing extremist sites which could suggest an interest in radicalisation.

9. General and Best Practice

- Think before you print; printing is expensive and consumes resources which is bad for the environment.

- Priority must be given to pupils wishing to use the computers for School use.

- Always log off your computer when you have finished using it.

- Always back up your work if you are not saving it on the School system. Work saved on the School system is backed up every night for you, but be careful if you only have a copy of your work on a memory stick or disk as you could lose it.

- Avoid saving or printing sizeable files (e.g. above 5mb); if in doubt ask a member of IT.

- If someone makes you an offer on the web or via email which seems too good to be true, it probably is.

- Observe Health and Safety Guidelines; look away from the screen every 10 minutes to rest your eyes and make sure your chair is positioned and adjusted to the correct height to the desk.

- Be considerate and polite to other users.

- Housekeep your email regularly by deleting old mail.

- Leave your computer and the surrounding area clean and tidy.

- If a web page is blocked that you feel you have a legitimate use for, please ask IT and it can instantly be unblocked if approval is given.

- The Internet can become addictive. If you feel you are spending too long on it, please ask a teacher or another member of staff for advice.

- If you are leaving the School, please ensure you have saved any files or email you wish to keep to a memory stick or CD to take home.

- If in doubt, ask a member of the ICT Department.

10. Other Electronic Devices

- The School's policy regarding other electronic devices is stated in the School's Mobile Phone Policy. Simply, we do not allow electronic devices in School. None of your personal devices, e.g., DS, mp3 player, Wii, or other is covered by the School's insurance and the School accepts no liability for them.
- All devices should be security marked and kept locked away where possible. This also includes items such as digital cameras and personal DVD players, etc.

11. Mobile Phones (Also see the Mobile Phone Policy)

- We have specific arrangements in place for the use of mobile phones. For the Middle and Senior Divisions, a mobile phone must not be used during lessons unless you have the teacher's permission.

- Similarly, do not take photos or videos with any device during lessons unless the member of staff has given permission.

- Do not take photos of people without their permission.

- Bullying by text or any other method will be treated in the same severe manner as any other form of bullying. This applies to all Divisions and extends to mobile phone activity OUTSIDE of School.

- Do not attempt to hack into someone else's device via Bluetooth or any other method. Bluetooth connectivity should be switched off when you are at School.

12. Music/Video Players (e.g. iPods)

- The use of such devices is banned during lessons unless the teacher has given permission.

- Do not connect such a device to the School network/School computers.

- Do not break copyright laws by swapping illegal music/video files.

- Do not listen to music in lessons whether via CDs or MP3, etc. unless the teacher has given permission.

Guidelines and Good Advice:

Guidelines on Cyber-Bullying

Cyber bullying is bullying which occurs through or with electronic media such as mobile phones, cameras, email, web sites etc. This could include any of the following:

- Bullying by texts or messages or calls on mobile phones
- Use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on web-sites
- Hi-jacking email accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat-rooms
- Posting threatening, abusive, defamatory or humiliating material on social networking sites.

Cyber-bullying can be more intrusive than other forms of bullying because it can occur 24 hours a day, 7 days a week and may be almost impossible for a victim to escape. HOWEVER – users are almost never totally anonymous online and it may be possible for the service provider (mobile phone company, web site or internet provider) to track the source. While cyber-bullying itself is not a criminal offence, a number of criminal offences may be committed in the course of cyber-bullying. From 1st July 2015 all school are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn in to terrorism. This is known as the Prevent duty. Schools must ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

How to avoid being thought of as a cyber-bully:
Before sending a message to anyone, or posting a comment on a web site about anyone, including your teachers, think whether you would be happy to receive such a message, or see such a comment about yourself. If not – don't do it.

Dealing with cyber-bullying:
All the normal rules for dealing with bullying apply in accordance with the Anti-bullying Policy. IN PARTICULAR if you are being bullied, or you know of someone else being bullied:

- Tell someone – a teacher, your housemistress, a member of the boarding staff, Matron, or a friend
- Report the incident on line by using the CEOPS icon which is on all school computers.

BUT

- NEVER reply or retaliate to bullying or abusive messages or images, or forward them to anyone. However they should be kept as evidence.

- NEVER give out personal details online

- NEVER give out passwords to your mobile, email or other online accounts.

Students should be aware of the following:

- The school reserves the right to monitor use of the internet on a routine basis and, if there is a good reason to do so, to examine mobile phones and other electronic devices and will, if necessary, delete inappropriate images or files

- Misuse of technology is subject to the school's disciplinary regime under the Behaviour and Discipline Policy and the Anti-bullying Policy

- They will be held personally responsible for all material they have placed on a web site and for all material that appears on a web site of which they are the account holder; misconduct of this kind outside school will be subject to school discipline if the welfare of other pupils or the culture or reputation of the school are placed at risk; and sanctions may include confiscation of mobile phones or restrictions on the use of the internet.

Some useful resources:

- http://www.dfes.gov.uk/bullying/pupilindex.shtml - cyber-bullying information
- http://www.stoptextbully.com/ - preventing text bullying
- http://www.chatdanger.com/ - general information on keeping online safe

Student Guidelines for Social Networking Sites Social networking sites such as Facebook provide dynamic new ways of communicating with friends and family around the world. However these sites can unintentionally expose far more personal details to the outside world than you would want. This could compromise your good name with potential employers or for further education, bring the School into disrepute or even provide opportunities for identity theft. The rapidly changing nature of these sites makes it difficult to give specific guidelines though the following are intended to help you avoid problems. Facebook is used as the example however the same principles should be applied to any other site that you use.

2. When you sign on for a Facebook account use your full name and add Ignore personal questions about sexuality, politics or religion that you may regret later in life.

3. Set your Profile privacy settings so that your personal details and postings are only visible to your friends. (To do this click on Privacy on the top menu bar of Facebook, then click on Edit Settings for Profile and set this to Only my friends and click on Save at the foot of the page.)

4. Set your Profile so that only your friends and some of your networks can find you (To do this return to Privacy, select Edit Settings for Search, select Only My Friends under 'Which Facebook users can find me' in search, and uncheck View your friend list under 'What Can People Do With My Search Results'). Otherwise anyone with access to your profile also has access to all your friends' profiles and they may not thank you for that, or you may not wish them to know with whom you are Facebook friends.

5. Do not agree to be friends with someone you do not know.

6. Do not put up embarrassing photos of yourself.

7. There are lots of exciting applications in Facebook and new ones are being added all the time. Do think carefully which ones you add – some have rather misleading names. E.g. Honesty box allows your friends to send you anonymous messages. This is not really an example of honesty and you are recommended not to use this sort of application.

8. If you decide to join a Group check the following first:

a. **Group type**
i. If this is global and open to anyone to join then look carefully at the postings before you decide to join. You will have no control over who reads what you write to this group.

ii. If the Group is closed then there will be some measure of control by the Administrators and you will have to apply to join the group.

b. **Title**
i. If the title is offensive to an individual or a group of individuals then stay away – these Groups are breaking Facebook's own rules.

ii. If the title is a spoof site (e.g. for a school or House or games team) then stay away – Groups such as this risk prosecution if the postings are libellous.

c. **Administrators**
i. If these are known to you, decide if you wish to be under their control on Facebook.

ii. If they are not known to you then consider even more carefully, and look at the type of postings on the group, before you become associated with it.

9. Do leave a Group if you are not happy with the type of postings – this avoids you being sucked into any investigation and subsequent action against the Group if it is deemed to be breaking Facebook's rules. If you join a group and then wish to leave you can do this easily by clicking on Leave Group in your list of My Groups.

10. Do be aware that if you decide to set up a Group you will be responsible for everything that is posted on that Group.

a. **Group Type -** the best setting for a Group is closed so that you approve all members.

b. **Group Title** and Description are visible to everyone with a Facebook account. If the title or description is defamatory of an individual or group of people then it could be cause for legal action on its own since it may incite members to post further defamatory or libellous comments and images.

c. **Enabling parts of the Group** - as Administrator you can disable any part of the Group so that non-members are not able to see these.

d. **Editing contributions** - as Administrator you are able and expected to delete any contributions which are inappropriate. Not to do so, renders you liable for the comments as well as the author.

e. **Editing Members** - as Administrator you are able to delete and even permanently ban any Group member who continues to use the site for abuse or other inappropriate postings.

f. **Leaving a Group** - if you decide to leave a Group that you have created then you can simply delete yourself as a member, but it would be prudent to transfer Admin rights to a friend you can trust – with their permission of course.

g. **Deleting a Group** - if a Group gets out of hand and you no longer wish to take responsibility for its existence you can close it down by deleting all members leaving yourself until last. When you delete the last member the Group disappears

A copy of this policy is available on the School website: www.beechwood.org.uk

(Reviewed September 2016 DHM)
Date of review September 2017