GRACE DIEU
MANOR SCHOOL

Acceptable Use Policy

School Mission Statement:

"Learning and growing in the light of the gospel"

WITHIN THE POLICY:

- Introduction
- SMART Rules
- Guidelines and Good Advice

Acceptable Use Policy

This policy relates to the use of technology, including:

- e-mail (outside of School as pupils do not have a personal School email)
- the internet
- social networking or interactive websites, for example Facebook, Twitter, MySpace, Ask Fm, Instagram, Snapchat and current trends of a similar format/nature
- instant messaging, chat rooms, blogs and message boards
- gaming sites (including online gaming*)
- mobile phones (including PDA and similar devices)
- mobile phones 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.

* *The Year 8 Xbox wireless connection has been disabled.*

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 is put at risk.

This Policy can be made available in large print or other accessible format if required.

Definitions:

Cyber-bullying is the use of information and communication technology (ICT), particularly mobile phones and the internet deliberately to upset someone else. (Frequency, severity, content will all be considered as to whether it constitutes cyber-bullying.)

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.

I**ntroduction**

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 you can report anything you are not happy about to anyone you feel you trust. This could be your Tutor, Mrs Burley, Mrs Kewell or Mr Fisher, parent or someone else's parent. **Tell someone.**

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 not** allowed in School. Permission may be given for certain events or activities but this will be made clear to pupils.

- 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, e.g., Facebook, email or Skype during lesson times. The School's *Social Networking Sites Policy* sets out our reasons in more depth, **but as a rule we do not allow access to such site at any time.** 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 a serious disciplinary matter**.

- Do not attempt to bypass School's 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 Grace Dieu Manor School 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.

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 another's credit card details 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.

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 a member pf 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 Mrs Burley.

- 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 homework 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.

- 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 food 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 Grace Dieu. **(See guidelines on Cyber Bullying below.)**

- 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. 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.

5. Privacy

- All files and emails on the system are the property of the School. As such, system administrator(s) (Mr Danvers and Mr Fisher) 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 (web based) on the School system are logged.

- If you are suspected of breaking this Policy, your own personal laptop/device and mobile telephone (should it be in School, although it ought not to be) can, albeit very rarely, 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.

6. 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.

7. 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 even expulsion.
- A breach of the law may lead to the involvement of the police.

8. 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 Mrs Burley.
- 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.
- 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 you wish to keep to a memory stick or CD to take home.

- If in doubt, ask Mrs Burley.

9. Other Electronic Devices

- The School's Policy regarding other electronic devices is that 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 brought into School should have permission, should (ideally) be security marked and kept locked away where possible or handed in for safe keeping. This also includes items such as digital cameras and personal DVD players, etc.

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.

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, Sister, Mrs Kewell, Mrs Burley or Mr Fisher

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 all with parents' knowledge and permission.

- Misuse of technology is subject to the School's disciplinary regime under the Behaviour 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 is placed at risk. Sanctions would be proportionate but could lead to the School invoking its more serious ones.

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

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.

(Reviewed August 2016 PSF)