Saint GREGORY'S
Bath

IT Acceptable Use Policy (Students)

Key Information

Title	IT Acceptable Use Policy (Students)	
Prepared By	Adrian Foley, Head of Computing	July 2023
Checked By	Karen Tyler, Data Manager Stuart Hodder, Network Manager	July 2023
Approved By	Governors' Christian Vision Committee	July 2023
Version	V01.02	
Document Update	July 2023	

Version History

Version	Date	Amendments
V01.00	July 2021	Approved by Governors
V01.01	June 2022	Split into separate documents for staff and students
V01.02	July 2023	Point made about Artificial Intelligence (ALIM)

"In Christ we flourish"

Contents

Appendix

Statement of intent

Whilst our school promotes the use of technology and understands the positive effects it can have on enhancing students' learning and community engagement, we must also ensure that technology is used appropriately. Any misuse of technology will not be taken lightly and will be reported to the Headteacher and the Deputy Headteacher Pastoral in order for any necessary further action to be taken in line with the school's Behaviour for Excellence policy.

This Acceptable Use Policy is designed to outline student responsibilities when using technology. It applies to all students using school IT facilities.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone.

These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

All users should have an entitlement to safe access to the internet and digital technologies at all times. This Acceptable Use Policy is intended to ensure:

- that students will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that students are protected from potential risk in their use of technology in their everyday studies.

The school will try to ensure that students have good access to digital technology to enhance learning opportunities. It will, in return, expect students to agree to be responsible users.

1. General policy and code of practice

1.1. The school has well-developed and advanced IT systems, which it intends for students to benefit from.

1.2. This policy sets out the rules that students must comply with to ensure that the system works effectively for everyone.

1.3. In order to protect students' safety and wellbeing, the school may view any data, information or material on the school's IT systems (whether contained in an email, on the network, in notebooks or on laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police.

Code of practice

The school's philosophy	In using IT, you will follow the school's ethos and consider the work and feelings of others. You must not use the system in a way that might cause annoyance or loss of service to other users.
User ID and password	You will be given your own user ID and password. You must keep these private and not tell or show anyone what they are. Your password must be at least eight characters in length and contain: • A mixture of lower case and upper case letters • At least one digit • At least one symbol If you forget or accidentally disclose your password to anyone else, you must change it. You must not use another person's account or allow another person to use your account. The facilities are allocated to you on a personal basis and you are responsible for the use of the machine when you are logged on. The school's system records, and senior IT staff monitor, your use of the system.
Logging on and off	You must log off from the computer you are using at the end of each of your sessions and wait for the standard login screen to reappear before leaving the computer.
Printing	You must ask your teacher before printing documents.
Access to information not normally available	You must not use the system or the internet to find or use facilities or flaws in the system that might give access to information or areas of the network not normally available. You must not attempt to install software to explore or harm the system. Use of hacking tools, e.g. 'loggers', 'sniffers' or 'evidence elimination software', is expressly forbidden.
Connections to the computer	You should use the keyboard, mouse and any headphones provided. You must not adjust or alter any settings or switches without first obtaining permission from a member of the IT staff. You must never attempt to use any of the connectors on the back of any desktop computer. You are not permitted to connect anything to the computer.

Virus	If you suspect that your computer has a virus, you must report it to your teacher or a member of the IT staff immediately.
Installation of software, files or media	You must not install or attempt to install software of any kind to network drives or local hard drives of networked desktop computers. You must not alter or re-configure software on any part of the school's system.
File space	You must manage your own file space by deleting old files rigorously.
Food and drink	You must not eat or drink, or bring food or drink, including sweets and chewing gum, into the IT rooms.

2. Internet policy and code of practice

2.1. The internet is a large and very useful source of information. Numerous websites and services, both official and unofficial, provide information or links to information which could be useful for educational purposes.

2.2. The school can provide access to the internet from desktop PCs via the computer network and through a variety of electronic devices connected wirelessly to the network.

2.3. Whenever accessing the internet using school equipment you must observe the code of practice below.

2.4. This policy and code of practice is designed to reduce and control the risk of offences being committed, staff or other students being offended and the school's facilities and information being damaged.

2.5. Any breach of this policy and the code of practice will be treated extremely seriously, and will be reported to the Headteacher and the Deputy Headteacher Pastoral.

Why is a code of practice necessary?

- Although there is much useful information on the internet, there is a great deal more material which is misleading or irrelevant. You will be taught how to use the internet effectively.
- Unfortunately, the internet carries a great deal of unsuitable and offensive material. It is important for legal reasons, reasons of principle and to protect staff and students who access the internet, that it is properly managed. Accessing certain websites and services, and viewing, copying or changing certain material, could amount to a criminal offence and give rise to legal liabilities.
- There is a danger of importing viruses on to the school's network, or passing viruses to a third party, via material downloaded from or received via the internet, or brought into the school on disks or other storage media.

Code of practice

Use of the internet	In school, the internet is provided for education use only.
Inappropriate material	You must not use the internet to access any newsgroups, links, list-servers, web pages or other areas of cyberspace that could be offensive because of pornographic, indecent, racist, violent, illegal, illicit, or other inappropriate content. You are responsible for rejecting any links to such material which may appear inadvertently during research. If you encounter any material which could be regarded as offensive you must leave that website or service immediately and not make any copy of that material. If you encounter any difficulty in leaving a website or service, you must inform your teacher immediately.
Misuse, abuse and access restrictions	You must not misuse or abuse any website or service or attempt to bypass any access controls or restrictions on any website or service.
Monitoring	The internet access system used by the school maintains a record which identifies who uses the facilities and the use that you make of them. The information collected includes which website and services you visit, how long you remain there and which material you view.
Giving out information	You must not give any personal information concerning anyone in the school when accessing any website or service.
Personal safety	You should take care who you correspond with. You should not disclose where you are or arrange meetings with strangers you have got in contact with over the internet.
Hardware and Software	You must not make any changes to any of the school's hardware or software. This prohibition also covers changes to any of the browser settings. The settings put in place by the school are an important part of the school security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage the school's systems.
Copyright	You should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. You must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits you to do so.

3. Email policy and code of practice

3.1. The school's computer system enables members of the school to communicate by email with any individual or organisation with email facilities throughout the world.

3.2. Any breach of this policy and code of practice will be treated seriously and will be reported to the Headteacher and the Deputy Head Pastoral.

3.3.

Code of practice

Purpose	You should only use the school's email system for school related emails.
Disclaimer	The school disclaimer that automatically appears at the end of each of your emails notifies the recipient that any email correspondence between you may be monitored. You must not remove this disclaimer.
Monitoring	Copies of all incoming and outgoing emails, together with details of their duration and destinations are stored centrally (in electronic form). The Network Manager has full access to all school emails. The frequency and content of incoming and outgoing external emails is monitored through Office 365 Malware. In school all machines are monitored and recorded through our School Monitoring system.
Security	As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents.
Program files and non-business documents	You must not introduce program files from external sources on to the school's network. This might happen by opening an email attachment or by downloading a file from a website. Although virus detection software is installed, it can never be guaranteed 100% successful, so introducing nonessential software is an unacceptable risk for the school. If you have any reason for suspecting that a virus may have entered the school's system, you must contact the IT support staff immediately.
Inappropriate emails or attachments	You must not use email to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work. You must not send personal or inappropriate information by email about anyone in the school community. If you receive any inappropriate emails or attachments you must report them to your teacher.
Viruses	If you suspect that an email has a virus attached to it, you must inform your teacher immediately.
Storage	All students must regularly delete emails they no longer require. Emails that you delete will be removed automatically from your "Deleted Items" Folder after 14 days.

4. Email policy – advice to students

Students should be guided by the following good practice:

- Check your school email accounts regularly;
- Always include a subject line when sending an email;
- Keep old emails for the minimum time necessary.

Student IT Agreement

I understand that I must use the school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

1. **For my own personal safety:**
   - I understand that the school will monitor my use of the systems, devices and digital communications.
   - I will keep my username and password safe and secure. I will not share them or try to use any other person's username and password. I will not write down or store my password where it is possible that someone may find it and use it.
   - I will be aware of 'stranger danger' when I am communicating on-line.
   - I will not disclose or share my name, my address, my email address, my mobile number, my age, my gender, my educational details or any other personal data about myself when on-line.
   - I will **NOT** arrange to meet up with people that I have communicated with on-line.
   - I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

2. **To ensure the safety and wellbeing of other users:**
   - I will not disclose or share their name, their address, their email address, their mobile number, their age, their gender, their educational details, any financial details or any other personal data about them when on-line.
   - I will not take or distribute images of anyone without their permission.
   - I will respect others' work and property and will not access, copy, remove or otherwise alter any other users' files.
   - I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

3. **I understand that everyone has equal rights to use technology as a resource and therefore:**
   - I understand that the school systems and devices are primarily intended for educational use and I will not use them for personal or recreational use.
   - I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

4. **I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school and therefore:**
   - I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
   - I will immediately report any damage or faults involving equipment or software.
   - I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email. I will not open any hyperlinks if I have any concerns about the validity of the email. This is due to the risk of the attachment containing viruses or other harmful programmes.
   - I will not install or attempt to install or store programmes of any type on any school device.
   - I will not try to alter computer settings.
   - If I am a sixth form student I am allowed to bring my own device (BYOD). I understand that if I do use my own devices in the school I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
   - If I am a Year 7 to 11 student I will not use my own personal devices on the school site.

5. **When using the internet for research, I recognise that:**
   - I should ensure that I have permission to use the original work of others in my own work
   - Where work is protected by copyright, I will not try to download copies (including music and videos)
   - When I am using the internet to find information, I should take care to check that the information that I access is accurate as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

6. **I will only use my school email account and the school's learning platforms (Microsoft Teams and Google Classroom) for school related work. When using these systems:**
   - I will ensure that I show respect and only send appropriate messages to both teachers and other students.
   - I will never use my school email account for distributing, accessing or storing images, text or materials that might be considered discriminatory, offensive or abusive. I will not send any email that is a personal attack, is sexist or racist, or might be considered as harassment or bullying.
   - I will produce work that will always be appropriate and will not use strong, aggressive or inappropriate language. I appreciate that others may have different opinions.
   - I will ensure that the work I produce and send through the school's learning platforms will never infringe upon copyright. I will always reference the work used.
   - I will never use the school learning platforms and my school email account for personal use or for sending chain letters, social media material or blogging inappropriate images, etc.
   - I will always ensure I do not use the school learning platforms to share personal information such as full names, locations, family information, phone numbers, etc.

7. **I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).**

8. **I will not use artificial intelligence language model (AILM), such as of ChatGPT, Bard, Bing or other similar tools for school related projects, homework or any school related tasks**.

9. **I will only use social media sites with permission and at the times that are allowed.**

10. **I understand that I am responsible for my actions, both in and out of school:**
    - I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
    - I understand that if I fail to comply with this Student IT Agreement I will be subject to intervention action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Name of Student: **Signature:**

Name of Parent/Carer: **Signature:**

Date: