**Information and Communications Technology Acceptable Usage Policy**

**Introduction**

The internet provides children and young people with a wealth of opportunities for their entertainment, communication and education. But there are also risks of harm through the deliberate behaviour of others online, and through exposure to inappropriate content. Pupils at primary school learn the principles for keeping safe online and this is developed at secondary school where they learn about the opportunities offered by the internet as well as the risks and their own responsibilities when working online. At St Bernard's Catholic Grammar School there are procedures in place to safeguard all learners from unlawful, sexual or otherwise potentially harmful content on the internet.

Computers and the internet are essential elements of 21st century life for education, business and social interaction. Information and Communications Technology (ICT) prepares students for a rapidly changing world in which many activities are transformed by access to a varied and constantly changing and developing technology. The school has a duty to provide students, who show a responsible and mature approach to its use, with quality Internet access as part of their learning experience.

The purpose of ICT systems and Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. It is a vital tool in the process of teaching and learning; students use ICT tools to find and process information. This needs to be done responsibly, creatively and with discrimination. Students learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of sources. All staff and students need to become confident users of ICT so that they can develop the skills, knowledge and understanding, which enables them to use appropriate ICT resources effectively as powerful tools for teaching, learning and administration.

At St Bernard's, the ICT systems are of approximately the same size and complexity as those of a medium sized company and it is necessary to have a formal policy on how these resources may be used, in order to protect students from unsuitable material, and to ensure the security and availability of those systems.

The School's Internet service filters the web sites students may visit; however, with the rapid growth of the Internet there is NO cast-iron guarantee that all sites containing offensive, extremist or unsuitable material will have been blocked. Provided students, monitored by staff, adhere to this policy then any risks of unsuitable material being accessed will be reduced to an absolute minimum.

This policy document should be discussed between both parent and student, and be signed by both on an annual basis, recognising its requirements, in order to be permitted to access the School's Internet and computer systems.

This Policy has been written by the school, building on the LEA policy and government guidance. It has been agreed by the senior management and approved by Governors.

This policy is in place for use of the school's ICT facilities by students; there is a separate policy for use by staff.

There are many computers available for use by students and the majority of these have access to the internet through the school network. All students have a login name, password and an email account. The email system is available for use both from within school and externally using a web browser, via the School's website. There are specialist ICT facilities serving Technology and Science departments together with general purpose rooms. A growing number of other computers are located within individual classroom areas.

The school takes responsibility for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that:

- Students can only access data to which they have right of access.
- No student be able to access another's files without permission.
- Access to personal data is securely controlled in line with the school's internal data security policy and as required by the General Data Protection Regulation (GDPR).
- Logs are maintained of access by students and of their actions while users of the system.

The internet provides people with a wealth of opportunities for their entertainment, communication and education. But there are also risks of harm. Considering the Prevent Duty in particular, there is a legal requirement for schools to have due regard to the need to prevent people being drawn into terrorism and the school has procedures in place to safeguard all students from unlawful, sexual, extremist or otherwise potentially harmful content on the internet.

**Students' use of the school's computer systems**

The facilities are provided to support and enhance curriculum-related activities. Each student will be issued with their own username and password, which must be kept confidential. Students must remember to log off when they have finished using the computer. It is good practice to change passwords regularly.

The following code of practice must be adhered to and signed by all students (see Appendix 1 for the ICT: Student acceptable usage agreement and Appendix 3 for the ICT: Use of personally owned devices by Sixth Form students). All visiting students are expected to sign the ICT: Visiting student acceptable usage agreement (see Appendix 2) and visiting Sixth Form students the ICT: Use of personally owned devices by visiting Sixth Form students agreement (see Appendix 4). Any student that uses the ICT provision within the school in a manner that falls outside of this code of practice is liable to face appropriate sanction, including the use of internal or fixed-term exclusion.

- The student's school email address must always be used for all school-related activity. Personal emails must not be used for any school-based activity.
- Emails are not confidential and can go astray; therefore email must not be used in any way that could potentially bring the school into disrepute.
- The use of another person's user name and password, use of abusive language, sending of abusive messages and changing of computer settings are not permitted and all will be considered serious offences.
- Students may not permit any other user to access the network via their password.

- Students may not damage, modify, or attempt to access other user's files or folders.
- Students must not copy, alter, print or change another student's work in any shape or form without the person's prior knowledge and consent. Please note that copyright regulations apply to electronic publications as they do to paper.
- Students must use the internet facilities only to support their school work, unless they have been given specific permission by a member of staff.
- Students should be aware that information on the internet may not always be reliable and sources should be checked. Also websites are used for advertising material, which may influence the contents.
- Students may not download or store any graphics or music files which are not directly related to school work. All such files may only be stored if students have received prior permission from the relevant member(s) of staff.
- Students may not download, store or run any executable files which have not been provided by the school, this includes games.
- Students may not send, store, display, post or intentionally access any offensive, pornographic, indecent, extremist or illegal material (this includes via mobile text messages).
- Students must not engage with any organisations over the internet which could be considered to support extremism, radicalisation or terrorism of any kind.
- Students must not send any chain email, or excessive quantities of or excessive sized emails. Nor must they use the ICT facilities to invade another's privacy.
- Students may not use any computer or communications services to harass, insult or bully other people (this includes mobile text messages).
- Students may not print any files which are not directly related to school work, and care should be taken to ensure effective use of limited printing resources.
- Students may not damage the hardware or attempt to delete or modify the installed software, or modify the operating system environment, including screensavers and wallpaper.
- Students may not attempt to access the school's server.
- Students may not violate copyright laws.
- Students may not use chat rooms or forums of any description via the school network unless given specific permission by a member of staff.
- Students must always adhere to the rules for the use of computer rooms at all times.
- No unauthorised computer, personal organiser, mobile or data processing device may be connected to the school network by any means, with the exception of students in the Sixth Form who are permitted to access the school's connection via Wi-Fi in the supervised study area.

- Students may not attempt to bypass the network security systems or firewalls by direct means or with the use of internet proxy servers.

- Students must not disclose to anyone on the internet their home address, telephone number, the name of the school or a photograph of themselves unless specific permission is given from a member of staff. Nor should they ever arrange to meet anyone they have met only via the internet unless this is part of a school project approved by their teacher.

- Students must never pretend to be anything or anyone that they are not and must be aware that the posting of anonymous messages is forbidden.

- Students must never engage in or respond to online bullying, suggestive or unpleasant emails or social media entries.

- Any student that sees something via the school's ICT provision that makes them feel worried or uncomfortable should report it immediately to a member of staff.

- Students are not allowed to damage the school's ICT provision, physically or otherwise, by:

    - Changing configuration or cabling unless specifically directed to do so by a member of staff.

    - Hacking of the school's or external systems. Students must be aware that hacking into computers is a criminal offence and they could be prosecuted under the Computer Misuse Act 1990.

    - Changing the contents of hard drives.

    - Bringing food or drink into computer areas or the vicinity of computers within classrooms.

**Responsibility**

Any student inadvertently accessing unsuitable material must immediately report it to an appropriate member of the school staff.

Any student becoming aware of access to undesirable material by any other person must immediately report that access to an appropriate member of school staff.

**Privacy**

The school reserves the right to monitor, inspect, copy, and review at any time and without prior notice computer and internet usage and all information transmitted or received in connection with such usage (for example emails). All such information, files, and images shall be and remain the property of the school and no student shall have any expectation of privacy in such material.

In the event of a serious security incident, the police may request, and will be allowed access to, a student's work area and usage history.

**Sanctions**

Failure to comply with any of the above may result in the following actions without prior notice.

a) Removal of Internet or computer access for a defined period, which could ultimately prevent access to files held on the system, including examination coursework.

b )Referral to Head of Year/Deputy Head/Head Teacher

c) Informing parent/guardian, and where required external agencies.

d) Other sanctions as outlined in the Behaviour policy, including exclusion on either a fixed-term or permanent basis.

If a student is found to engage with any organisations over the internet which could be considered to support extremism, radicalisation or terrorism of any kind then the matter will be reported to the Designated Lead for the school (Mike Tomlinson) or the Headteacher, who have a legal obligation to report it to the local authority.

**Monitoring and evaluation**

Governors need to ensure that appropriate filters and monitoring systems are in place on the school's ICT resources. They also are required to ensure that staff have regular safeguarding training, including online safety training, and that students are taught about e-safety, for example, through personal, social, health and economic education. This policy will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

**Reviewing**

The efficacy of the policy will be discussed as part of the Governors' rolling programme of reviews. It should be read in conjunction with the following policies:

- Behaviour policy.
- E-safety policy.
- ICT policy.
- Safeguarding & Child Protection policy.

**Agreed by the Catholic Life of the School Committee: 27th January 2021**

**Review Date: Spring 2023**

**APPENDIX 1**

**ICT: Student acceptable usage agreement**

Access to the school network and internet is provided for you to carry out recognised schoolwork. This provision will only be made on the understanding that you agree to follow the guidelines outlined below:

- Computer file storage areas are treated as school property. ICT staff may look at files and communications to ensure that the system is being used responsibly. I understand that my work and emails are not private.
- I am aware that a member of the ICT staff could view my computer screen, from the school network at any time.
- I understand that I am responsible for good behaviour and that general school rules apply whilst using the computers.
- I understand that eating or drinking in the computer rooms or near a computer are strictly prohibited.
- I will not reveal my password to anyone. If I think someone knows my password, then I will change it.
- I will not use another person's password. If I am doing shared work, I will email a copy to my own work area.
- I will not copy, alter, print or change another student's work in any shape or form without the person's prior knowledge and consent.
- I understand that programs must not be loaded or installed on a computer except by ICT staff. I will not bring programs in on removable media, email or download them from the internet.
- I understand that the use of the internet is a privilege and provided for students to conduct genuine research only to support their school work, unless they have been given specific permission by a member of staff.
- I understand that all the internet sites that I visit are recorded.
- I understand that I must not download any files without permission.
- I understand that I must not access social media or messaging apps (such as WhatsApp, Instagram, SnapChat, TikTok) whilst using school computers.
- I understand that I must not use chat rooms, play games, mobile ring tones sites or SMS sites whilst using school computers.
- I understand that I must not use web mail, other than that provided for my school account.

- I understand that I must not use obscene or offensive language. I will remember that communication should be polite to maintain the good reputation of the school.
- I understand that I must not seek out any offensive, pornographic, indecent, extremist or illegal material.
- I understand that I must not seek out any organisations over the internet which could be considered to support extremism, radicalisation or terrorism of any kind.
- I understand that I must not complete mailing lists or subscription forms on the internet for personal use whilst using school computers.
- I understand that I must not violate copyright laws. (Never copy and make use of any material without giving credit to the author. Copyright, Designs & Patents Act 1988). If I am unsure then I will ask a member of staff for advice.
- I understand that I must not attempt to hack into the computer systems of the school or any other external systems. I am aware that hacking into computers is a criminal offence and that I could be prosecuted under the Computer Misuse Act 1990.
- I understand that I may not print any files which are not directly related to school work.
- I understand that I may not attempt to access the school's server.
- I understand that I may not attempt to bypass the network security systems or firewalls by direct means or with the use of internet proxy servers.
- I understand that I must not disclose to anyone on the internet my home address, telephone number, the name of the school or a photograph myself unless specific permission is given from a member of staff. Nor will I ever arrange to meet anyone that I have met only via the internet unless this is part of a school project approved by my teacher.
- I understand that I must never pretend to be anything or anyone that I am not and must be aware that the posting of anonymous messages is forbidden.
- I understand that I must not send any chain email, or excessive quantities of or excessive sized emails and that I must not use the ICT facilities to invade another's privacy.
- I understand that I must never engage in or respond to online bullying, suggestive or unpleasant emails or social media entries.
- I understand that if I see something via the school's ICT provision that makes me feel worried or uncomfortable that I should report it immediately to a member of staff.
- I understand that I must not damage the school's ICT provision, physically or otherwise, by:
    - Changing configuration or cabling unless specifically directed to do so by a member of staff.
    - Changing the contents of hard drives.

**Sanctions**

- I understand that violations of the above rules will result in appropriate sanction. These sanctions are outlined in the school's Behaviour Policy and may include exclusion, whether internal or fixed-term.

- I understand that I am always subjected to the Data Protection Act, the General Data Protection Regulation, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.

The School reserves the right to seek reimbursement from parents of students who cause malicious damage to ICT equipment.

During lessons, teachers will guide students toward appropriate materials. However, outside school, families bear this responsibility.

---

Please sign both copies - return one copy to the school and retain the second copy for your records.

**We agree to the terms and conditions of the ICT: Student acceptable usage agreement.**

Name of student:…… Tutor group: ……

Student's signature:…… Date: ……

Parent/Carer's signature: …… Date: ……..

**APPENDIX 2**

**ICT: Visiting student acceptable usage agreement**

As a visitor to St Bernard's Catholic GS, we ask that you act sensibly and appropriately in your use of the school's ICT provision and network. Access to the school network and internet is provided for you to carry out recognised schoolwork. This provision will only be made on the understanding that you agree to follow the guidelines outlined below:

- Computer file storage areas are treated as school property. ICT staff may look at files and communications to ensure that the system is being used responsibly. I understand that my work and emails are not private.
- I am aware that a member of the ICT staff could view my computer screen, from the school network at any time.
- I understand that I am responsible for good behaviour and that general school rules apply whilst using the computers.
- I understand that eating or drinking in the computer rooms or near a computer are strictly prohibited.
- I will not reveal my password to anyone. If I think someone knows my password, then I will change it.
- I will not use another person's password. If I am doing shared work, I will email a copy to my own work area.
- I will not copy, alter, print or change another student's work in any shape or form without the person's prior knowledge and consent.
- I understand that programs must not be loaded or installed on a computer except by ICT staff. I will not bring programs in on removable media, email or download them from the internet.
- I understand that the use of the internet is a privilege and provided for students to conduct genuine research only to support their school work, unless they have been given specific permission by a member of staff.
- I understand that all the internet sites that I visit are recorded.
- I understand that I must not download any files without permission.
- I understand that I must not access social media or messaging apps (such as WhatsApp, Instagram, SnapChat, TikTok) whilst using the computers at St Bernard's School.
- I understand that I must not use chat rooms, play games, mobile ring tones sites or SMS sites whilst using school computers.
- I understand that I must not use web mail, other than that provided for my school account.
- I understand that I must not use obscene or offensive language. I will remember that communication should be polite to maintain the good reputation of the school.

- I understand that I must not seek out any offensive, pornographic, indecent, extremist or illegal material.
- I understand that I must not seek out any organisations over the internet which could be considered to support extremism, radicalisation or terrorism of any kind.
- I understand that I must not complete mailing lists or subscription forms on the internet for personal use whilst using school computers.
- I understand that I must not violate copyright laws. (Never copy and make use of any material without giving credit to the author. Copyright, Designs & Patents Act 1988). If I am unsure then I will ask a member of staff for advice.
- I understand that I must not attempt to hack into the computer systems of the school or any other external systems. I am aware that hacking into computers is a criminal offence and that I could be prosecuted under the Computer Misuse Act 1990.
- I understand that I may not print any files which are not directly related to school work.
- I understand that I may not attempt to access the school's server.
- I understand that I may not attempt to bypass the network security systems or firewalls by direct means or with the use of internet proxy servers.
- I understand that I must not disclose to anyone on the internet my home address, telephone number, the name of the school or a photograph myself unless specific permission is given from a member of staff. Nor will I ever arrange to meet anyone that I have met only via the internet unless this is part of a school project approved by my teacher.
- I understand that I must never pretend to be anything or anyone that I am not and must be aware that the posting of anonymous messages is forbidden.
- I understand that I must not send any chain email, or excessive quantities of or excessive sized emails and that I must not use the ICT facilities to invade another's privacy.
- I understand that I must never engage in or respond to online bullying, suggestive or unpleasant emails or social media entries.
- I understand that if I see something via the school's ICT provision that makes mefeel worried or uncomfortable that I should report it immediately to a member of staff.
- I understand that I must not damage the school's ICT provision, physically or otherwise, by:
    - Changing configuration or cabling unless specifically directed to do so by a member of staff.
    - Changing the contents of hard drives.

**Sanctions**

- I understand that violations of the above rules will result in appropriate sanction. These sanctions are outlined in the school's Behaviour Policy and may include exclusion, whether internal or fixed-term.

- I understand that I am always subjected to the Data Protection Act, the General Data Protection Regulation, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.

The School reserves the right to seek reimbursement from parents of students who cause malicious damage to ICT equipment.

During lessons, teachers will guide students toward appropriate materials. However, outside school, families bear this responsibility.

---

Please sign both copies - return one copy to the school and retain the second copy for your records.

**I agree to the terms and conditions of the ICT: Visiting student acceptable usage agreement.**

Name of student:…… School: ……..

Student's signature:…… Date: ……

**APPENDIX 3**

**ICT: USE OF PERSONALLY OWNED DEVICES BY SIXTH FORM STUDENTS**

**Introduction**

This policy is in place for the occasions when students use their own ICT equipment in school.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled.
- Logs are maintained of access by users and of their actions while users of the system.

When students use their own devices (eg laptops, tablets, smartphones) it is imperative that:

- The protocols already in use are maintained.
- No vulnerabilities are introduced into the school's existing secure environments.
- Data protection matters are complied with.
- All BYODs must have appropriate security in place and it must be updated regularly. It is the staff member's responsibility to ensure this.
- Periodic audits and checks on compliance will be undertaken by the school's network manager, who is also available to offer guidance on what is and is not acceptable use of BYODs.
- It is essential to be careful when installing any third-party software onto a BYOD. Untrusted sources have the potential to contain malware which could compromise any personal material belonging to the school. If in doubt, consult the network manager before uploading.

**Misuse of BYODs by students**

Misuse or abuse of the facility to use BYODs by students is a serious matter and will be dealt with under the school's disciplinary procedures.

**Monitoring and evaluation**

The headteacher may request access to personal devices if the senior leadership team considers that this policy has been contravened, in order to investigate alleged abuse.

**ICT: Student acceptable BYOD usage agreement**

- I will always adhere to copyright.
- I will always log off the system when I have finished working.
- I will only access the school's systems with my own name and registered password.
- Passwords that I use to access school systems will be kept secure and secret.

- If I have reason to believe my password is no longer secure, I will change it immediately. I will inform the network manager as soon as possible so that any access with my old password can be monitored and appropriate action taken.
- I understand that when in school and not being used, the BYOD must be kept safely in my locker or about my person and at my own risk. It must not be left unattended.
- **The BYOD must be covered by my parents 'normal household insurance.**
- I understand that I have the responsibility to ensure the virus protection software that has been installed is kept up-to-date. I also understand that I must *always* follow the virus protection procedures as directed by the school's network manager to ensure virus protection is always kept up-to-date.
- I will follow the guidance provided by ICT support staff to ensure the anti-virus protection on my BYOD is kept up-to-date.
- If I use removable media I will ensure that this has been carefully checked to ensure it is free from any type of virus.
- I understand that I may load software onto the BYOD but it must:
  - Be fully licensed.
  - Not corrupt any software or systems already installed on the BYOD.
  - Not affect the integrity of the school networks when connected to either the curriculum or networks.
- **I understand that the school may monitor my BYOD activity.**
- I understand that activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

I understand that if I do not adhere to these rules outlined in this agreement, my privilege of working with the BYOD could be suspended and other disciplinary consequences may follow.

If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may require investigation by the police and could be recorded on any future criminal record checks.

---

Please sign both copies - return one copy to the school and retain the second copy for your records.

**We agree to the terms and conditions of the ICT: Use of Personally Owned Devices by Sixth Form Students agreement.**

Name of student:…… Tutor group: ……

Student's signature:…… Date: ……

Parent/Carer's signature: …… Date: ……..

**APPENDIX 4**

**ICT: USE OF PERSONALLY OWNED DEVICES BY VISITING SIXTH FORM STUDENTS**

**Introduction**

This policy is in place for the occasions when students use their own ICT equipment in school.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled.
- Logs are maintained of access by users and of their actions while users of the system.

When students use their own devices (eg laptops, tablets, smartphones) it is imperative that:

- The protocols already in use are maintained.
- No vulnerabilities are introduced into the school's existing secure environments.
- Data protection matters are complied with.
- All BYODs must have appropriate security in place and it must be updated regularly. It is the staff member's responsibility to ensure this.
- Periodic audits and checks on compliance will be undertaken by the school's network manager, who is also available to offer guidance on what is and is not acceptable use of BYODs.
- It is essential to be careful when installing any third-party software onto a BYOD. Untrusted sources have the potential to contain malware which could compromise any personal material belonging to the school. If in doubt, consult the network manager before uploading.

**Misuse of BYODs by students**

Misuse or abuse of the facility to use BYODs by students is a serious matter and will be dealt with under the school's disciplinary procedures.

**Monitoring and evaluation**

The headteacher may request access to personal devices if the senior leadership team considers that this policy has been contravened, in order to investigate alleged abuse.

**ICT: Student acceptable BYOD usage agreement**

- I will always adhere to copyright.
- I will always log off the system when I have finished working.
- I will only access the school's systems with my own name and registered password.
- Passwords that I use to access school systems will be kept secure and secret.

- If I have reason to believe my password is no longer secure, I will change it immediately. I will inform the network manager as soon as possible so that any access with my old password can be monitored and appropriate action taken.
- I understand that when in school and not being used, the BYOD must be kept safely in my locker or about my person and at my own risk. It must not be left unattended.
- **The BYOD must be covered by my parents 'normal household insurance.**
- I understand that I have the responsibility to ensure the virus protection software that has been installed is kept up-to-date. I also understand that I must *always* follow the virus protection procedures as directed by the school's network manager to ensure virus protection is always kept up-to-date.
- I will follow the guidance provided by ICT support staff to ensure the anti-virus protection on my BYOD is kept up-to-date.
- If I use removable media I will ensure that this has been carefully checked to ensure it is free from any type of virus.
- I understand that I may load software onto the BYOD but it must:
  - Be fully licensed.
  - Not corrupt any software or systems already installed on the BYOD.
  - Not affect the integrity of the school networks when connected to either the curriculum or networks.
- **I understand that the school may monitor my BYOD activity.**
- I understand that activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

I understand that if I do not adhere to these rules outlined in this agreement, my privilege of working with the BYOD could be suspended and other disciplinary consequences may follow.

If an incident is considered to be an offence under the Computer Misuse Act or the Data Protection Act this may require investigation by the police and could be recorded on any future criminal record checks.

---

Please sign both copies - return one copy to the school and retain the second copy for your records.

**We agree to the terms and conditions of the ICT: Use of Personally Owned Devices by Sixth Form Students agreement.**

Name of student:…… School: ……

Student's signature:…… Date: ……