

ICT & Internet Acceptable Use Policy

St Bernard's High School



Approved by: Full Governing Body

Date: June 2023

Last reviewed on: June 2023

Next review due by: June 2027

Contents

1. Introduction and aims	3
2. Relevant legislation and guidance	4
3. Definitions	3
4. Unacceptable use.....	4
5. Staff (including Governors, volunteers and contractors)	5
6. Students.....	8
7. Parents.....	9
8. Data security.....	9
9. Protection from cyber attacks	9
10. Internet access	11
11. Monitoring and review	12
12. Related policies.....	12
Appendix 1: Social cheat sheet for staff	13
Appendix 2: Acceptable use of the internet: agreement for parents and carers.....	15
Appendix 3: Acceptable use agreement for students	17
Appendix 4: Acceptable use agreement for staff, Governors, volunteers and visitors	19
Appendix 5: Cyber security glossary....	20

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our School works, and is a critical resource for students, staff (including Senior Leadership Teams), Governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the School.

However, the ICT resources and facilities our School uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of School ICT resources for staff, students, parents and Governors
- Establish clear expectations for the way all members of the School community engage with each other online
- Support the School's policy on Data Protection, Online Safety and Safeguarding
- Prevent disruption to the School through the misuse, or attempted misuse, of ICT systems
- Support the School in teaching students safe and effective internet and ICT use

This policy covers all users of our School's ICT facilities, including Governors, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Disciplinary Policy and Procedure, Behaviour Policy, Cyber Bullying Policy and Staff Code of Conduct

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- [Data Protection Act 2018](#)
- [The General Data Protection Regulation](#)
- [Computer Misuse Act 1990](#)
- [Human Rights Act 1998](#)
- [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)
- [Education Act 2011](#)
- [Freedom of Information Act 2000](#)
- [The Education and Inspections Act 2006](#)
- [Keeping Children Safe in Education 2021](#)
- [Searching, screening and confiscation: advice for Schools](#)
- [National Cyber Security Centre \(NCSC\)](#)
- [Education and Training \(Welfare of Children Act\) 2021](#)

3. Definitions

- **ICT facilities:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or

service which may become available in the future which is provided as part of the ICT service

- **Users:** anyone authorised by the School to use the ICT facilities, including Governors, staff, students, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose
- **Authorised personnel:** employees authorised by the School to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

See Appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the School's ICT facilities by any member of the School community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the School's ICT facilities includes:

- Using the School's ICT facilities to breach intellectual property rights or copyright
- Using the School's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the School's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the School, or risks bringing the School into disrepute
- Sharing confidential information about the School, its students, or other members of the School community
- Connecting any device to the School's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the School's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the School's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the School
- Using websites or mechanisms to bypass the School's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way.

This is not an exhaustive list. The School reserves the right to amend this list at any time. The Head Teacher or any other relevant member of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the School's ICT facilities.

4.1 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the School's policies on Disciplinary Policy and Procedure, Behaviour Policy, Anti Bullying Policy and Staff Code of Conduct

5. Staff (including Governors, volunteers, and contractors)

5.1 Access to School ICT facilities and materials

The School's HR manage access to the School's ICT facilities and materials for School staff referring to the PA to the Head Teacher for authorisation to set up individuals and their access rights. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the School's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact HR.

5.1.1 Use of phones and email

The School provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the School has provided.

Staff must not share their personal email addresses with parents and students, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the SLT members responsible for GDPR immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or students. Staff may use personal phones to conduct work-related business but following already published guidance

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

The School can record in-coming and out-going phone conversations.

Callers **must** be made aware that the conversation is being recorded and the reasons for doing so and the School phone system is set up to notify callers

Staff who would like to record a phone conversation should speak to the IT technicians in the first instance

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

Currently only Reception are set to automatically record conversations in the event that the conversation needs to be referred to in the subsequent days. They automatically delete after 30 days.

5.2 Personal use

Staff are not permitted to use School ICT facilities for personal use

Staff may not use the School's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Where School's facilities are used for personal reasons, staff should be aware they may put personal communications within the scope of the School's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) when in their office, Staff Room but not in the presence of students except for educational purposes

Staff should be aware that personal use of ICT (even when not using School ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where students and parents could see them.

Staff should take care to follow the School's guidelines on social media (see Appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The School has guidelines for staff on appropriate security settings for social media accounts (see Appendix 1).

5.3 Remote access

We allow staff to access the School's ICT facilities and materials remotely.

The School has a public website, hosted by FSE Design where there is a tab that allows access to the VLE which is a Microsoft SharePoint platform. This is managed by the School.

Access is given when staff and students join the School and access to areas is dependent upon the individual's role in the School. IT Technicians and named individuals are able to access individual Teams

The VLE is an Office 365 programme and so stored in the cloud.

Users should always be mindful of their access to the system whether in School or outside. Passwords should never be disclosed; equipment should never be left unattended with programmes open and others should not be allowed sight or access to School based programmes or information

If a member of staff requires additional access they should initially ask their line manager

Staff accessing the School's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the School's ICT facilities outside the School and take such precautions as all may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

The School's Data Protection Policy can be found on the VLE, Staff, Policies.

5.4 School social media accounts

The School has official Instagram/Facebook/YouTube/X and LinkedIn pages, managed by the Social Media Co-ordinator. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The School has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of School network and use of ICT facilities

The School reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The School monitors ICT use in order to:

- › Obtain information related to School business
- › Investigate compliance with School policies, procedures and standards
- › Ensure effective School and ICT operation
- › Conduct training or quality control exercises
- › Prevent or detect crime
- › Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

6. Students

6.1 Access to ICT facilities

- › Computers and equipment in the School's ICT suite are available to students only under the supervision of staff"
- › Specialist ICT equipment, such as that used for Music, or Design and Technology, must only be used under the supervision of staff
- › Students will be provided with an account linked to the School's virtual learning environment, which they can access from any device via the public website
- › Sixth form students can use the computers/personal devices in their Common Room and the Sixth Form Study Area independently for educational purposes only. Where they use personal devices rather than School laptops their usage will not be monitored. The School firewall will be able to detect what had been accessed but would have to be viewed, it would not send any alerts. It would however prevent access to sites already flagged as inappropriate.
- › Some students may be invited to use a device when in a lesson by their teacher.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's [guidance on searching, screening and confiscation](#), the School has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under School rules or legislation.

The School can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the School's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse contains an online element.

6.3 Unacceptable use of ICT and the internet outside of School

The School will sanction students, in line with the School policies if a student engages in any of the following **at any time** (even if they are not on School premises):

- › Using ICT or the internet to breach intellectual property rights or copyright
- › Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- › Breaching the School's policies or procedures

- › Any illegal conduct, or statements which are deemed to be advocating illegal activity
- › Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- › Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- › Activity which defames or disparages the School, or risks bringing the School into disrepute
- › Sharing confidential information about the School, other students, or other members of the School community
- › Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- › Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the School's ICT facilities
- › Causing intentional damage to ICT facilities or materials
- › Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- › Using inappropriate or offensive language.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the School's ICT facilities as a matter of course.

However, parents working for, or with the School in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the School's facilities at the Head Teacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the School online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the School through our website and social media channels.

We ask parents to sign the agreement in Appendix 2.

8. Data security

The School is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the School cannot guarantee security. Staff, students, parents and others who use the School's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the School's ICT facilities should set strong passwords for their accounts and keep these passwords secure. (Currently 8 characters including upper and lower case, a number and special symbol)

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

All staff are encouraged to use a password manager to help them store their passwords securely. Teachers reset student passwords when forgotten.

At the start of each Autumn term all staff are forced to reset their network password. School provided laptops force staff to reset the device password periodically. Where staff have access to other programmes such as SIMS it is recommended that they regularly change their password. Staff should have a different password for SIMS from their network password.

8.2 Software updates, firewalls and anti-virus software

All of the School's ICT devices that support software updates, security updates and anti-malware products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the School's ICT facilities.

Any personal devices using the School's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the School's Data Protection Policy.

The School's Data Protection Policy can be found [VLE/Staff/policies/Data Protection](#).

8.4 Access to facilities and materials

All users of the School's ICT facilities will have clearly defined access rights to School systems, files and devices.

These access rights are managed by the IT Technicians

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT Technicians immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The School ensures that its devices and systems have an appropriate level of encryption.

School staff are allowed to use personal devices (including computers) to access School data or work remotely using the School portal.

Laptops provided by the School are provided with an encryption key that must be inserted when turning on but stored separately when machine is left unattended.

USB's (memory sticks, pen drives) should not be used in the School.

Where examination coursework has to be sent to examination boards in this format specific permission and guidance must be sought from the IT Technicians.

9. Protection from cyber attacks

Please see the glossary (Appendix 6) to help you understand cyber security terminology.

The School will:

- Work with Governors and the IT department to make sure cyber security is given the time and resources it needs to make the School secure
- Provide annual training for staff in the form of a video from the NCSE and regular phishing simulations (and include this training in any induction for new starters, if they join outside of the School's annual training window) on the basics of cyber security, including how to:
 - Check the sender address in an email
 - Respond to a request for bank details, personal information or login details
 - Verify requests for payments or changes to information.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
 - **Proportionate:** the School will be looking to develop a relationship with a third-party with a view to objectively test that what it has in place is up to scratch
 - **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe
 - **Up-to-date:** with a system in place to monitor when the School needs to update its software
 - **Regularly reviewed and tested:** to make sure the systems are as up to scratch and secure as they can be.
- Arranges for on site and Office 365 data is backed up daily. There is secondary back up of the Office 365 data. Sims data is also backed up to the Cloud. All onsite data is backed up to a server held in a different building. Finally there is an annual backup, stored on a hard drive in a fireproof safe.
- Manages SIMS on site with support from ESS
- Ensure staff access the School system from outside the School via the VLE using their various passwords
- Make sure ICT staff conduct regular access reviews to make sure each user in the School has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Develop, review and test an incident response plan with the IT department, for example, including how the School will communicate with everyone if communications go down, who will be contacted when, and who will notify [Action Fraud](#) of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)'

10. Internet access

The School wireless internet connection is secured.

- Through filtering
- There are separate connections for staff/students/ the public

10.1 Students

- WiFi is available to all students. Where using laptops the usage will be managed by the member of staff. Students are not allowed to use their own devices unless in the sixth form where they are working independently and in agreed areas or where specifically managed by a member of staff
 - The firewall (Fortigate) will impose restrictions ➤
- The WiFi allows access to School equipment.

10.2 Parents and visitors

Parents and visitors to the School will be permitted to use the School's guest WiFi when invited to by specific event organiser/member of staff

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The SLT will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the School.

This policy will be reviewed every year with the Governing Body responsible for approving this policy.

12. Related policies

This policy should be read alongside the School's policies on:

- Safeguarding and Child Protection
- Behaviour
- Disciplinary Policy and Procedure
- Data Protection
- Cyber Security
- Social Media Policy
- Staff Code of Conduct
- Anti Bullying

Don't accept friend requests from Students on Social Media

Appendix 1: Social Media cheat sheet for staff

10 rules for School staff on Social Media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your students
6. Don't use social media sites during School hours
7. Don't make comments about your job, your colleagues, our School or your students online – once it's out there, it's out there
8. Don't associate yourself with the School on your profile (e.g. by setting it as your workplace, or by 'checking in' at a School event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app and potentially other apps from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or students).

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – for Facebook go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What to do if...

A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify Senior Leadership and/or their parents. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the Senior Leadership Team or the Head Teacher about what's happening.

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
 - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the School
 - Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.

AGREEMENT FOR LAPTOP USE BY STUDENTS

The laptop is owned by the school and is for the use of the student to further their education. This Agreement applies at all times, in and out of school hours, and has been drawn up to protect all parties – students, staff and the school.

The school reserves the right to examine and/or delete any files that may be held on the laptop and/or to monitor its use. No food, drink or snacks are to be consumed anywhere near the laptop.

All students are required to sign a copy of the Code of Practice.

AGREEMENT

I understand and agree to abide by the following rules:

- a) Any activity or use of the laptop which threatens its integrity, or attacks or corrupts it or any other system, is forbidden;
- b) Use of the laptop for personal financial gain, gambling, political purposes or advertising is forbidden;
- c) Copyright requirements of materials must be respected;
- d) Students must not:
 - o Attempt to delete system or application files, or modify system or work station settings;
 - o Attempt to gain access to unauthorised areas of the laptop;
 - o Download games or executable files.

I acknowledge receipt of a _____

I accept responsibility for the safe keeping and care of this machine, and undertake to return it for all required upgrades. Upon leaving the school, I undertake to return the laptop and all its accessories on or before my last day at the school.

Student's Full Name: _____ Form: _____

Signed (Student): _____ Date: _____

Acceptable use of the internet: agreement for parents and carers

Name of parent/carers:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our School.

The School uses the following channels:

- Our official Facebook page
- Email/text groups for parents (for School announcements and information)
- Our virtual learning platform

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the School via official communication channels, or using private/independent channels to talk about the School, I will:

- Be respectful towards members of staff, and the School, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the School's official channels, so they can be dealt with in line with the School's complaints procedure

I will not:

- Use private groups, the School's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the School can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the School's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other students. I will contact the School and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:

Date:

Appendix 3: Acceptable use agreement for students

Code of Conduct for ICT, Internet and Mobile Devices

The computer network and associated ICT equipment, including student laptops and Virtual Learning Environment, are owned by the school and may be used by students to further their education. This Code of Conduct applies at all times, in and out of school hours, and has been drawn up to protect all parties – students, staff and the school.

The school reserves the right to examine and/or delete any files that may be held in any part of the computer system and to monitor the use of the Internet by students. Very strong action will be taken against any student visiting inappropriate Internet sites and/or using email in such a way that it intimidates or bullies another person (see Cyberbullying Policy and Mobile Devices Policy on the school website).

All students are required to sign a copy of this Code of Conduct. Refer to full details of the Policy.

Social Media

Any social networking that has a negative impact on the school or its community will result in appropriate sanctions and possible Police intervention. Any posting of images taken at school, or on school trips, will lead to appropriate sanctions. It is a criminal offence for any student to send or hold any indecent images of students via any form of technology, e.g., the internet, mobile phone, etc. Such an activity can result in permanent exclusion.

Mobile Devices Policy – new updated information is below

Mobile Devices (information is also in Student Booklet)

As part of our ongoing process in reviewing our policies and procedures, St Bernard's High School will be changing the mobile phone policy in light of parental comments.

These changes will be made in all relevant school policies and the planner which your daughter/son will be issued with.

First time

If your daughter/son is found to be using their mobile phone in school or the phone is not switched off (for Sixth Form this would be outside the common room), the mobile phone will be kept until the end of the school day and a Head of Year detention will be issued with a letter sent home.

Your daughter/son will be able to collect their mobile phone from Reception at the end of the school day.

Second time (within the same term)

If your daughter/son is found to be using their mobile phone in school or the phone is not switched off for a second time within the same term (for Sixth Form this would be outside the Common Room), the mobile phone will be kept for two school days and a formal detention will be issued with a letter sent home.

Your daughter/son will be able to collect their mobile phone from Reception at the end of the second day.

For example, if their mobile phone was confiscated on the Monday, they will be able to collect their mobile phone on Wednesday at the end of the school day.

If their mobile phone was confiscated on the Friday, your daughter/son would not be able to collect their phone until Monday at the end of the school day. More than two times (within the same term)

If your daughter/son is found to be using their mobile phone in school or it is not switched off more than two times within the same term (for Sixth Form this would be outside the common room), the mobile phone will be kept for one week and a letter will be sent home.

The parent/carer will have to collect the mobile phone from reception a week from when it was confiscated.

For example, if their mobile phone was confiscated on the Monday, the parent/carer will be able to collect their mobile phone the following Monday at the end of the school day from Reception.

If your daughter/son's mobile phone is to be kept for two days or the week, the school will send a message to you via school comms.

FOR SIXTH FORM

The sixth form has an "off and away during the day" mobile phone policy. You will only be allowed to use your phones at break or lunch in the sixth form common room, at all other times it should be "off and away." This will be enforced using the mantra of "see it, hear it, loose it." If a phone is seen outside of the sixth form area at any point it will be confiscated even if this is the first offence.

Why do we do this, because the science tells us that smartphone usage:

- Reduces reaction times, task performance, task enjoyment, retention of learning, and academic outcomes.

- Increases disruptive behaviour, academic dishonesty, depression, stress, anxiety, (cyber-) bullying, and contributes to poor quality sleep.

The computer network and associated ICT equipment, including student laptops and Virtual Learning Environment, are owned by the school and may be used by students to further their education. This Code of Conduct applies at all times, in and out of school hours, and has been drawn up to protect all parties – students, staff and the school.

The school reserves the right to examine and/or delete any files that may be held in any part of the computer system and to monitor the use of the Internet by students. Very strong action will be taken against any student visiting inappropriate Internet sites and/or using email in such a way that it intimidates or bullies another person (see Cyberbullying Policy and Mobile Devices Policy on the school website).

All students are required to sign a copy of this Code of Conduct. Refer to full details of the Policy.

Students must use their devices sensibly when in school. We have an off and away during the day policy, as already stated above. Students can use their phones in the common room only. If they are found using them outside the common room they will be confiscated, and students can collect their phone from reception at the end of the school day.

If this happens a second time within the same term it will be confiscated, and the parent will be asked to come and collect the phone after a week. An SLT detention will also be set.

Students can only use their devices if instructed by a member of staff, they should never assume they can use them.

Any misuse of their phones within supervised study will result in an immediate confiscation of the phone and an SLT detention logged. We make it clear to students that they should be using their devices in a responsible way in supervised study

Digital Communication with Staff

When contacting staff, students should use their school email account only. Formal standard English should be used in all communications when using their school email account.

CODE OF CONDUCT FOR I.T. and INTERNET USE BY STAFF

All Staff

The computer network and associated IT equipment, including staff laptops and the Virtual Learning Environment, "the computer system" is owned by the school. It is for the use of staff to enhance their professional activities including teaching, research, administration and management. This Code of Conduct applies at all times, in and out of school hours, and has been drawn up to protect all parties – students, staff and the school.

Staff must not allow any student, or other person, to use their school network account under any circumstances; the sharing of accounts is strictly prohibited. Staff must keep their password confidential and should report immediately to the ICT Technicians if they suspect that another person has accessed their account. This applies to accessing the school network; school virtual learning environment and SIMS remotely. When accessing SIMS remotely, it will require 2 passwords - one for the school system and one for SIMS. These should be kept confidential and should be different to each other. Staff are expected to follow the best practice advice for password setting. This would involve:

- Setting a password that is at least 8 characters including upper and lower cases, numerals and a special character
- Not using the same password for every account
- Not related to family, personal details or anything easily guessable including references to work
- Not writing them down, or keeping a record separate from the equipment
- Consider using a password manager.

To enable staff to effectively organise their time, access to SIMS remotely has been authorised. However, the responsibilities around data protection remain.

It is the responsibility of a member of staff to ensure data accessed through SIMS is kept confidential and that no other person / persons can access their SIMS homepage and data. If staff suspect another person has accessed their SIMS area, the Head Teacher must be informed immediately.

The school reserves the right to examine and/or delete any files that may be held in any part of the computer system and/or to monitor the use of the Internet by staff. Very strong action will be taken against any member of staff visiting inappropriate Internet sites and/or using the computer system inappropriately, with the potential for dismissal in the most serious of cases.

When using the Internet, staff should be aware that information may be inaccurate or biased and it should be verified using other sources, if possible. Staff need to consider carefully any requests to provide personal information about students or other members of staff.

The school is not responsible for the consequences of any personal use of the computer system, in particular any transactions carried out. You are accountable for any actions taken on a machine connected to the computer network and/or to the internet, in your user name.

In the event of accidentally accessing inappropriate material, while using the laptop on the Internet or via e-mail, this should be reported to the Head Teacher at the earliest opportunity.

To safeguard staff and students, the use of personal mobile devices which access the internet and / or record images is not allowed; staff must not use personal equipment as part of learning activities. Images of students (for e.g. working / participating in activities / in classrooms) should never be taken with personal devices. School devices are available if events need to be recorded.

Action will be taken if staff are found to have student images / personal details on their mobile devices.

Personal mobile devices (e.g. phones, tablets, etc) should be used only in staff social time (lunchtime, pre and post school hours). School devices should not be used for social purposes. (Ref Social Networking Policy)

All members of staff are required to sign a copy of this Code of Practice and return it to the PA to the Head Teacher.

GUIDANCE ON STAFF LAPTOP USAGE

Laptop Care

Laptops are more fragile than desktop machines and require more care, in particular:

- Be careful not to bump or drop your laptop, do not carry items with it that could harm it and do not put any objects on top of it;
- When transporting your laptop always turn it off and use the carrying case;
- Avoid touching the screen;
- Avoid subjecting the laptop to extreme temperature changes;
- Keep all liquids and food away from your laptop;
- Whenever possible, avoid turning off your laptop when the hard drive light is on because your data could be lost or corrupted;
- Do not leave your laptop on overnight.

Laptop Security

In order to ensure that the laptops and the data they contain are appropriately protected:

- They should not be left on view in an unattended vehicle, nor left in a vehicle overnight;
- They should not be positioned so as to be visible from outside a ground floor window, unless there is no alternative;
- When leaving a laptop unattended for any extended period i.e. lunch break or overnight, it should ideally be locked away securely or placed in the most secure location available;
- If your laptop is stolen or lost, you must immediately advise the Police, the School Business Manager and the ICT technicians; this will ensure that recovery procedures can be started as soon as possible;
- Encryption USB key must not be kept with your laptop.

Laptop Access Control

- When you first receive your laptop, the default user password should be changed immediately on first logging in with the laptop – please refer to the Code of conduct for IT and Internet use by staff for guidance on passwords;
- You will be asked to change your password periodically;
- If the password is keyed in incorrectly 5 times, the user will be locked out of the system for 30 minutes before the user can try again - during the school day, the ICT department can override this;
- All school computers, including laptops, should always be locked (windows Key and L) whenever they are left unattended;
- You should ensure your user password and SIMS password are different.

Laptop Software

- The use of unlicensed software is illegal and should not be installed;
- Executable software must be approved by the IT staff before being installed;
- If you are installing files from outside sources such as the internet, these should be virus scanned before loading them on to your laptop. It is your responsibility to keep files having any form of virus off your laptop and potentially the school network;
- The school's IT staff will not support any software loaded on to laptops that:
 - has not been authorised;
 - is for personal use.
- Laptops should be logged on to the school's computer network at least every week, to ensure Software and windows is regularly updated.

Backing Up Your Work

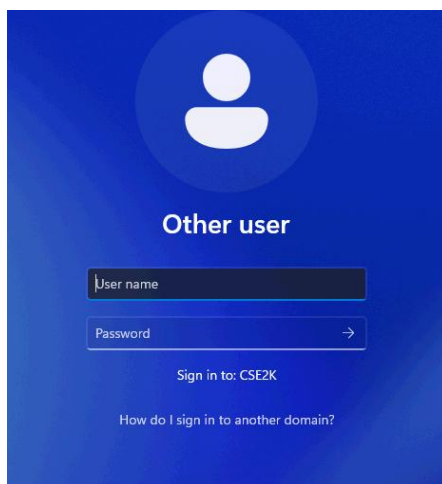
The following applies to those laptops that have not been set up with synchronisation, which are the majority of the machines.

If you are using your laptop out of school and not connected to the school network, you need to log on to the local machine using the details that was provided with your laptop

Ideally you should always connect to the schools virtual learning environment when out of school. By doing this your work will always be saved to the cloud and backed up. Only when this option is not available should work be saved to the laptop – please note this work will not be backed up. You should not be using a memory stick as these are prone to carry malware.

When you are back in school and connected to the school network, copy any work you have done when not connected to the network into your 'One Drive' directory. This will then automatically be uploaded to your One Drive and be available both in school and at home.

If you are using your laptop in school connected to the school network, you need to log on to 'CSE2K', as shown below.



AGREEMENT

I understand and agree to abide by the following rules:

- e) All Internet usage should be appropriate to the professional activities of staff;
- f) Use of the computer system to access illegal or inappropriate materials such as pornographic, racist or other offensive material is forbidden;
- g) Access to the computer system must only be made via a member of staff's authorised account and password, which should not be made available to any other person;
- h) Any activity or use of the computer system which threatens its integrity, or attacks or corrupts it or any other system, is forbidden;
- i) Staff are responsible for all e-mail material sent from their account and for any contacts made as a result of e-mail being received;
- j) As e-mail can be mis-directed, staff are required to use the same high standard of language and content as they would for letters or public communication;
- k) Use of the computer system for personal financial gain, gambling, political purposes or advertising is forbidden;
- l) Copyright requirements of materials must be respected;
- m) Members of staff must not:

- Attempt to delete system or application files, or other staff materials, or modify system or work station settings;
- Attempt to gain access to unauthorised areas of the computer system or another user's work area;
- Knowingly transfer malware to the network.

Full Name: _____ Dept: _____

Signed: _____ Date: _____

STAFF PROVIDED WITH SCHOOL LAPTOP COMPUTER

Upon Issuing the Laptop:

I acknowledge receipt of a _____ laptop computer, Serial No.

I accept responsibility for the safekeeping and care of this machine and undertake to return it for all required upgrades or any other work required. Upon termination of my contract with the school, I undertake to return the machine and all its accessories on, or before, the last day of my employment.

Signed: _____ Date: _____

Upon Return of the Laptop:

Confirmation that the above laptop computer was returned on _____

Signed: _____ Date: _____

Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the School will put in place. They're from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
Anti-malware	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying

TERM	DEFINITION
	out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.