St. Benet's Catholic Primary School

Acceptable Use Policy

Headteacher: Mr David Miller
Chair of Governors: Mrs Bernadette Davison
Date: May 2022
Date for Review: May 2023

'A happy and holy place of learning and the centre of a thriving community'

Acceptable Use Policy

Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom.

The internet is an essential element in 21st Century life for education and social interaction. The purpose of internet use in school is to promote pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration system. Benefits include:

- Access to worldwide resources and research materials.
- Educational and cultural exchanges between pupils worldwide (i.e. Skype).
- Access to experts in many fields.
- Staff professional development such as access to online learning and forums.
- Communication with support services, professional associations and colleagues.
- Exchange of curricular and administration data (i.e. between colleagues, LA and DfE).

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Consequently, in delivering the curriculum teachers need to plan to integrate the use of ICT and web-based resources including e-mail to enrich learning activities. Effective internet use is an essential life skill.

Access to the school's ICT network and use of ICT facilities owned by the school, including access to the Internet, are conditional on observance of the following Acceptable Use Policy. The Aims of this Acceptable Use Policy are to:

- Allow all users access to school ICT resources and use of the Internet for educational purposes.
- Provide a mechanism by which staff and pupils are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
- Provide rules which are consistent, and in agreement with the General Data Protection Regulation 2018, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.
- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.
- Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

The Acceptable Use policy governs the use of the School's corporate network that individuals use on a daily basis in order to carry out business and curricular functions.

This policy should be read in conjunction with the other policies in the School's Online Safety Policy.

Scope

This Acceptable Use Policy applies to all school employees and pupils, any authorised agents working on behalf of the school, including temporary or agency employees, and third-party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper.
- Information or data stored electronically, including scanned images.
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer.
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card.
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops.
- Speech, voice recordings and verbal communications, including voicemail.
- Published web content, for example intranet and internet.
- Photographs and other digital images.

Email
St Benet's Catholic Primary School provides email accounts to employees to assist with performance of their duties.

Personal Use
Whilst email accounts should primarily be used for business functions, incidental and occasional use of the email account in a personal capacity may be permitted so long as:

- Personal messages do not tarnish the reputation of the school.
- Employees understand that emails sent to and from corporate accounts are the property of the school.
- Employees understand that school management may have access to their email account and any personal messages contained within.
- Employees understand that the Emails sent to/from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation.
- Employees understand that the school reserves the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network.
- Use of corporate email accounts for personal use does not infringe on business functions.

Inappropriate Use
The school does not permit individuals to send, forward, or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files
- Unwelcome propositions
- Profanity, obscenity, slander, or libel
- Ethnic, religious, or racial slurs
- Political beliefs or commentary
- Any messages that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Other Business Use
Users are not permitted to use emails to carry out their own business or business of others. This includes, but not necessarily limited to: work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of school management.

Email Security

Users will take care to use their email accounts in accordance with the school's information security policy. In particular users will:

- Not click on links in emails from un-trusted or unverified sources.
- Use secure email transmission methods when sending personal data.
- Not sign up to marketing material that could jeopardise the school's IT network.
- Not send excessively large email attachments without authorisation from school management and the school's IT provider.
- Not forward e-mail messages onto others unless the sender's permission is first obtained.
- Not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive.

Internet Use for Staff

St Benet's Catholic primary School provides internet access to employees to assist with performance of their duties.

Personal Use

Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the school.
- Employees understand that school management may have access to their internet browsers and browsing history contained within.
- Employees understand that the school reserves the right to suspend internet access at any time.
- Use of the internet for personal use does not infringe on business functions.

Inappropriate Use

St Benet's Catholic Primary School does not permit individuals use the internet in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. The use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990). Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic images, cartoons, jokes or movie files.
- Images, cartoons, jokes or movie files containing ethnic, religious, or racial slurs.
- Any content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Individuals are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use

Users are not permitted to use the internet to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of school management.

Internet Security
users will not click on links to un-trusted or unverified Web Pages. Staff, Governors and Pupils must agree to and sign the Acceptable Use Agreement at the start of their employment/term of office. Visitors are asked to sign an acceptable use agreement when entering school.

Internet use for Pupils
Pupils who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material.

Pupils must have returned a signed consent form before being allowed to use the ICT facilities that involve accessing the internet. The school will keep a record of the returned forms which will regularly referred to by teachers and monitored by the Headteacher and admin staff.

Pupils must not use the school ICT facilities without the supervision of a member of staff and ICT facilities are not available when an adult is not present. Although use of the ICT facilities and access to the Internet will be supervised, and all possible measures will be taken (including the use of BWCET firewall), St Benet's Catholic Primary School and Bishop Wilkinson Catholic Education Trust cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

St Benet's Catholic Primary School is protected by the internet filtering company Smoothwall. This is live monitoring system which monitors and screen shots any inappropriate material viewed on a school computer. This material can be used as evidence in circumstances where a computer has been used to access such inappropriate material.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT subject leader and school office who will pass information onto the ICT Technician immediately who will, in turn, record the address and report on to the Headteacher, ICT services and Internet Service Provider. Through e-safety lessons, pupils must be made are aware of the following:

- They must only access those services they have been given permission to use.
- They must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.
- The use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990).

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Social Media Use
The school recognises and embraces the benefits and opportunities that social media can contribute to an organisation. The School also recognises that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

Personal Accounts
St Benet's understands that many employees will use or have access to Personal Social Media Accounts. Employees must not use these accounts:

- During working hours,
- Using corporate equipment,
- To conduct corporate business,
- To contact or approach clients, customers, or partners of the School.

Staff who use social media must ensure that their security settings are adjusted to safeguard themselves and the school. The Leadership Team will monitor the privacy of staff social media accounts termly. Staff must ensure:

- Their profile is private – all settings 'just friends'.
- Profile picture and cover photo are deemed appropriate.
- They do not 'like' or 'share' any inappropriate content (for example, racism, sex, extreme views and radicalisation).
- Any references to school, both stated and implied are not made at any time. This includes photographs or written statements.
- That no photographs are taken anywhere in the school on personal devices during teaching hours and that no photographs linked to school are uploaded on social media.

General Equipment Safety

The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals.

Users must treat with respect equipment and services in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities.

Legal Requirements

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please speak to the Headteacher. A Data Protection Impact Assessment will need to be carried out for all new software that is installed on the Schools IT systems. Remember also that shareware is not freeware and must be licensed for continued use.

Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a programme into the random-access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium.

The high cost of commercially marketed software and the ease with which it can be copied make it tempting to copy software illegally. Agents for software developers are aggressively seeking to protect their rights under the law. Schools can be audited at any time. Anyone found to have unauthorised copies of software will immediately be suspended from using the IT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability whatsoever.

"Hacking" is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Sanctions for Pupils

If pupils break the rules as laid down by this policy, they will lose temporary or permanent use of the school systems. Parents will be informed and if the law has been broken the police will be informed and the school will assist the police with any prosecution.

Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, the Disciplinary Policy outlines the correct procedures. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

Local Authority Designated Officer (LADO) - Managing Allegations:

The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Cyber Bullying (*see Anti-Bullying Policy*)

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through various media children can be cyber bullied 24 hours a day.
- People who cyber bully may attempt to remain anonymous.
- Anyone of any age can cyber bully.
- Some instances of cyber bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient.

Prevention of Cyber Bullying

St Benet's recognise that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe ICT practice into all our teaching and learning, incidents can be avoided.

The school is very reactive to the issues highlighted in the media and strives to ensure that children are educated on these matters before issues arise. Parents are involved in these occasions through parent workshops, drop in sessions or distributed information. Our community's principles of e-safety are based on "Key Safety Advice – Cyber Bullying' (DCSF 2007).

We recognise we have a shared responsibility to prevent incidents of cyber bullying but the Headteacher has the responsibility for coordinating and monitoring the implementation of anti-cyber bullying strategies.

Understanding Cyber Bullying

The school community is aware of the definition of cyber bullying and the impact cyber bullying has.

Staff receive guidance and review the Anti-Bullying and Acceptable Use Policies regularly. Children are taught how to recognise cyber bullying and their responsibilities to use ICT safely. ICT safety is integral to teaching and learning practice in the school.

Parents are also taught how to recognise cyber bullying and their responsibilities for supporting safe ICT use. The school provides regular parental updates on online safety and an online safety advice section on its website.

Cyber Bullying Record Keeping and Monitoring Safe Practice

As with other forms of bullying, the Headteacher keeps records of cyber bullying on CPOMS and in SIMS. Incidents of cyber bullying will be followed up using the same procedures as other forms of bullying. However, we recognise that monitoring internet use on a regular basis is a disincentive for bullies misusing school equipment and systems. The ICT technician will conduct regular use checks, log any concerns and inform the Headteacher.

Online Safety

Children and staff are reminded of what constitutes exemplary 'Online Safety Code of Conduct' at the start of each academic year.

- Under no circumstances should you give out personal email or postal addresses or telephone numbers of any person, including the staff and pupils at the school.
- Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by pupils and staff as they can result in degradation of service for other users and they are inappropriate and do not adhere to our school rules.
- Do not download, use or upload any material that is copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material.
- Users should assume that ALL software is subject to copyright restrictions, including shareware. Pupils must not, under any circumstances download or attempt to install any software on the school computers. Staff should seek the advice of the Headteacher if they would like to download or upload software.
- Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material of violent, dangerous, racist, or inappropriate sexual content. If users are unsure about this, or any materials, users must ask teachers or ICT coordinator. If in doubt, DO NOT USE. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.
- Search engines (such as Google) are not to be used to search for websites or images unless the learning objective specifically demands it.

Use of the School Network

- Always respect the privacy of files of other users.
- Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.
- The ICT technician and subject leader will view any material pupils store on the school's computers.
- Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year. Users unsure of what can be safely deleted should ask their subject leader or ICT technician for advice. In exceptional circumstances, increased storage space may be allowed by agreement with the ICT technician.
- Users accessing software or any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only. Visitors will receive a guest login that limits access to the network.
- Be polite and appreciate that other users are entitled to differing viewpoints. The use of strong language, swearing or aggressive behaviour is forbidden. Do not state anything that could be interpreted as libel.
- If the network is accessed from home, this Acceptable Use Policy applies.

General Security Guidelines

Backups

Files stored on the network are backed up every evening. This means files can be restored if deleted or lost in error. However, if you create and delete files on the same day then a backup will not be available to restore. Backups are kept securely on the school site in a fire proof safe.

Save Regularly

It is very important to save work regularly (approx. every 10 minutes). The network is very reliable but problems do occur i.e. programs crash, power failures. If work is saved regularly and a PC or the network does fail for any reason, only the work done since the last save will be lost. If you are working in Office 365, a copy of your document is saved automatically to the cloud.

Use your Network Area

Always ensure that files are saved to your network area, NOT on the local hard drive (your C drive). This will ensure that your work is backed up and can be retrieved in the event of a hardware failure or theft.

Personal Documents

The school cannot accept responsibility for personal documents held on school equipment.

Offsite pupil data and pupil information

USB sticks may not be taken off site. Staff must access the school systems remotely or use One Drive (Office 365) to transfer information between home and school. SIMS Teacher App may be used on a staff iPad to access data through a secure system when working from home.

Virus Checks

All computers in school have anti-virus software, although very new viruses will not be found. If you suspect a virus please report it to the ICT technician straight away and/or record in the ICT problem book if ICT Technician is not available.

Mobile Devices

- Pupils are not permitted to bring mobile phones or devices in to school. Should there be a need for a child to bring their device in to school this should be turned off and placed in plastic wallets in classrooms for the duration of the day.
- Any pupil who is seen with a mobile device during the school day will have their phone removed from them to be collected at the end of the school day (in accordance with the school's Behaviour Policy). The device will be secured in the school safe.
- Pupils may not make or take personal calls or send/receive text messages or social media messages from a mobile phone during the school day.
- Mobile phones may not be used to take pictures of pupils and staff (use class cameras/iPads provided by the school).
- Any inappropriate use of mobile devices, such as cyber bullying, during the school day must be reported to the Headteacher (see Cyberbullying).
- Staff should only use their mobile phones at appropriate times of the day only e.g. break times. During the school day their mobiles should be turned off or set to silent. These devices must be kept in a secure area away from areas where children access. Staff must not use personal mobile devices or cameras to take images of pupils or staff.

School Telephone Use

Personal Use

Whilst the telephone should primarily be used for business functions, incidental and occasional use of the telephone in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the school.

- Employees understand that school management may have access to call history.
- Employees understand that the school reserves the right to suspend telephone usage at any time.
- Use of the telephone for personal use does not infringe on business functions.

Inappropriate Use

The school does not permit individuals to use the telephone in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other Business Use

Users are not permitted to use the telephone to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of school management.

Video-Conferencing and Webcams

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

Managing Allegations against Adults Who Work with Children and Young People

In order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies we will refer to the Headteacher. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff. Allegations made against a member of staff should be reported to the Senior Designated Lead (SDL) for safeguarding within the school immediately. In the event of an allegation being made against a Headteacher, the Chair of Governors should be notified immediately.

Local Authority Designated Officer (LADO) - Managing Allegations:

The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

Additional Information

When pupils and employees leave St Benet’s Catholic Primary School, their user account and any associated files and email address and any associated emails will be removed from the school system and will no longer be accessible. The school cannot continue to receive emails sent to an email address that has been disabled.

If pupils, staff or parents do not understand any part of this Acceptable Use Policy, please ask the Headteacher and subject leader for further guidance.

A copy of this policy can be accessed by visitors via our school website.

Named Personnel
Our Named Governor for ICT Acceptable Use is Mrs Bernadette Davison

The Person Responsible for Online Safety and Acceptable ICT Use is Mrs Catherine Wealleans

Monitoring and Reviewing
This policy will be reviewed on an annual basis.
This policy was reviewed by Governors on: May 2022

St Benet's Catholic Primary School

KS1 Pupil's Acceptable Use Policy

'The best interests of the child must be a top priority in all things that affect them'.
Article 3 of the United Nations Convention on the Rights of the Child.

Young people are entitled to access to technology to help ensure that they can achieve their potential in their learning.

Young People are not entitled to abuse technology by deliberately attempting to interfere with the performance of the school or agency systems or devices belonging to other people.

Young People are not entitled to use devices and Internet services to have a negative impact on other people. This includes cyber bullying, Hyper Link to bullying site of any members of their school community, or wider community or have inappropriate access to other people's files and documents on the school or agency systems and the Internet.

Young People will abide by the following code of conduct:

- I will check with a grown up before using the internet.
- I will tell a grown up if something I see makes me feel worried.
- If I get stuck or lost on the internet I will ask for help.
- I can write polite and friendly messages to people I know.
- I will keep my personal information, my name, address, my school, my pictures "Top Secret" and not share it on an app or website.
- If I need to bring a mobile phone to school, I will hand it to the office for safe keeping until the end of the school day.
- I will not bring a tablet to school.

Name: ………………………………………………………………………………………………..

Signed: ……………………………………………………………………………………………

Date: ……………………………………………………………………………………………….

St Benet's Catholic Primary School

KS2 Pupil's Acceptable Use Policy

'The best interests of the child must be a top priority in all things that affect them'.
Article 3 of the United Nations Convention on the Rights of the Child.

Young people are entitled to access to technology to help ensure that they can achieve their potential in their learning.

Young People are not entitled to abuse technology by deliberately attempting to interfere with the performance of the school or agency systems or devices belonging to other people.

Young People are not entitled to use devices and Internet services to have a negative impact on other people. This includes cyber bullying, Hyper Link to bullying site of any members of their school community, or wider community or have inappropriate access to other people's files and documents on the school or agency systems and the Internet.

Young People will abide by the following code of conduct:

For my own personal safety…

- I will ask permission from a member of staff/adult before using the Internet.
- I am aware of "stranger danger" when I am communicating on line.
- I will never arrange to meet someone or give any personal information over the Internet (name, address, telephone number, name and address of school, bank or credit card details).
- I will tell an adult about anything online which makes me feel uncomfortable.
- I will only E-mail people I know, or who have been approved.
- I will report any unpleasant material (including on the internet) or messages sent to me. I understand this report would be confidential and would help protect other young people and myself.
- I will not attempt to bypass the system security to access material which is not permitted by my school.
- I understand that the school/agency may check my computer files and activity and may monitor the Internet sites I visit.
- I will be very careful when sharing pictures or video of myself or my friends, if I am in school I will always check with a teacher
- I will not put my "Personal Information" online. (My full name, birthday, phone number, address, postcode, school etc.)

To keep the system safe…

- I will only access the system with my own login and password, which I will keep secret.
- I will not allow other people to use my logon or password.
- I will not access other people's files.
- I understand that the ICT systems are primarily for educational use and I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not bring to school/agency any devices, to connect to the network or internet, from outside school unless I have been given permission.
- I will only use my own devices (including mobile phones PDAs, cameras, games consoles) when permitted and only for activities acceptable to the school
- I will not install software without permission

- I will not try to download or upload large files without permission which may make the system slow for other users
- I will not use the system for on-line gaming, on-line gambling, internet shopping, file sharing or video broadcasting without permission.

Responsibility to others:

- The messages I send will be polite and responsible.
- I understand that it is not acceptable to post or distribute images or video of other people without their permission.
- Where work is copyrighted (Including music, videos and images) I will not either download or share with others.
- I understand that the organisation may take action against me if I am involved in incidents of inappropriate behaviour wherever their location. If the activities are illegal this may be reported to the police.

Personal Devices:

- The school cannot accept responsibility for loss or damage to personal devices
- It is not permitted for pupils to use Mobile Phones during the school day. Phones should be handed in to the office at the beginning of the school day and collected at the end
- Other devices (e.g. Games consoles, cameras) should only be brought into school with permission from a teacher.

Name: ………………………………………………………………………………………………………..

Signed: ……………………………………………………………………………………………………

Date: ……………………………………………………………………………………………………….

Staff and Governors Acceptable Use Policy

'The best interests of the child must be a top priority in all things that affect them'.
Article 3 of the United Nations Convention on the Rights of the Child.

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

Colleagues must ensure that they fully understand that the consequences of inappropriate activity can be severe, leading to dismissal and criminal proceedings.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, tablets, digital cameras, email and social media sites.

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. Staff mobile phones are allowed in school, but should only be used for communication when not working with children. Staff mobile phones should not be used during lessons or when children are present.

4. Cameras on personal phones or tablets will not be used to take pictures of children in any circumstances.

5. I understand that any hardware and software provided by my school for staff use can only be used by members of staff.

6. Personal use of school ICT systems and connectivity is only permitted with the consent of the headteacher, outside of the school day.

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

8. I will respect system security and I will not disclose any password or security information. Log in passwords should be changed on a regular basis to improve security and prevent inappropriate use of school systems.

9. It is not permitted to use another person's log in details. On occasions when log ins are shared the details of this will be recorded in an e safety log or similar document.

10. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager. No device will be introduced to IT systems without ensuring it is free from malware, inappropriate/illegal content.

11. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place. All photographs and videos of children should therefore be stored on the school staff shared area. Any personal data which is being removed from the school site should be stored securely and used appropriately. Encrypted memory sticks will be used at all times especially when any pupil information (reports, assessment data, personal data, photographs etc.) is taken off site. Unencrypted memory sticks should not be used on school computing devices.

12. I will not keep professional documents which contain school-related personal information (including images, files, videos etc.) on any personally owned devices (such as laptops, digital cameras, mobile phones).

13. If I choose to use a portable device (Phone, Tablet etc…) to collect my work e-mail I will ensure that the device is locked by a pin code or password and will be wiped when I dispose of the device.

14. Digital Images or videos of pupils will only be taken from the school premises using encrypted memory sticks.

15. I will not use unapproved cloud storage systems (Dropbox, icloud etc) for storing personal data of staff or pupils.

16. I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

17. I will respect copyright and intellectual property rights. Where work is copyrighted (Including music, videos and images) I will not either download or share with others.

18. I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media.

19. I will not communicate with pupils or ex-pupils under the age of 18 using social media without the express permission of the Headteacher.

20. My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team. This would include any relatives of current pupils that are my “friends” on a social media site.

21. My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

22. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, BWCET, or the County Council, into disrepute. This would include any comment made, even in the belief that it is private on social media.

23. I will report all incidents of concern regarding children’s online safety to the Designated Child Protection Coordinator and/or the eSafety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator or the designated lead for filtering as soon as possible.

24. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team as soon as possible.

25. I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

26. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Computing Subject Leader or the Headteacher.

27. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School’s Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service’s information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

Name: ……………………………………………………………………………………………………..

Signed: ………………………………………………………………………………………………………

Date: …….

St Benet's Catholic Primary School

Visitors Acceptable Use Policy

'The best interests of the child must be a top priority in all things that affect them'.
Article 3 of the United Nations Convention on the Rights of the Child.

This is not an exhaustive list and all visitors are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1. I understand that Information Systems and ICT include not only the school's computers, but also any personally owned equipment such as a phone or tablet and its use on social media such as Facebook or Instagram.

2. Visitor mobile phones must be turned off unless specific permission has been obtained for their use from the Headteacher. Cameras on personal phones or tablets will not be used to take pictures of children in any circumstances.

3. Pupils and their families have a reasonable expectation of privacy so I confirm that I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have written permission from the Headteacher.

4. I will not communicate with pupils or ex-pupils under the age of 18 using social media without the express written permission of the Headteacher

5. I will not give my personal contact details such as email address, mobile phone number, IM account details to any pupil or parent in the school. Contact will always be through a school approved route. I will not arrange to VC or use a web camera with pupils unless specific permission is given.

6. While in the school my use of ICT and information systems will always be compatible with the ethos of the school, and if I am any doubt I will check this with a member of staff.

7. I understand that I have a duty of care to ensure that students in school use all forms of electronic equipment and devices safely and should report any inappropriate usage to a senior member of staff.

8. Visitors are requested not to contact a parent of a child directly, but to go through the school's official channels.

9. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

Name: ……………………………………………………………………………………………………..

Signed: ……………………………………………………………………………………………………

Date: ……………………………………………………………………………………………………….