Acceptable Use Policy

Contents

Staff, Volunteers and Pupils

At all Blessed Christopher Wharton Catholic Academy Trust schools', we understand the importance and benefits of using computers to help with children's learning and personal development. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies may include use of devices, for example tablets, cloud computing, learner owned devices which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

We ask all pupils, volunteers, governors, visitors and staff (referred to as staff throughout this policy) involved in the life of the Trust to sign an Acceptable Use Policy (AUP). The Acceptable Use Policy is intended to ensure:

- that staff, volunteers and pupils will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use and understand how we expect them to behave when they are online.
- that Trust school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.
- support the Trusts' policy on data protection, online safety and safeguarding.

Blessed Christopher Wharton Catholic Academy Trust understands it has a legal and professional obligation to include online safety as part of our wider safeguarding responsibilities. As such, will try to ensure that staff have good access to ICT to enhance their work, to enhance learning opportunities and will, in return, expect staff, volunteers, governors and pupils to agree to be responsible users. Further information can be found in our Online Safety Policy.

Relevant 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 2020
- Searching, screening and confiscation: advice for schools

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.

Unacceptable use of a school's ICT facilities includes:

- Using a school's ICT facilities to breach intellectual property rights or copyright.
- Using a school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the Trust/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.
- Activity which defames or disparages the Trust or a school, or risks bringing the school into disrepute.
- Sharing confidential information about the Trust, school, its pupils, or other members of the school community
- Connecting any device to a school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Trust or schools' 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 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 Trust or a school.
- Using websites or mechanisms to bypass the filtering mechanisms.

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. Staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of our ICT facilities.

Where the use of our ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Trust discretion.

Sanctions

Anyone working on behalf of the Trust who engage in any of the above unacceptable activities may face disciplinary action in line with the Trust or school policies: behaviour, discipline, staff discipline, staff code of conduct, online safety.

Acceptable Use Staff

Staff should understand that they must use Trust/school systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the systems and other users. They will recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. Staff will, where possible, educate the young people in their care in the safe use of digital technology and embed online safety in their work with young people.

Access to Trust ICT facilities and materials

The Trust/individual school manages access to their ICT facilities and materials on behalf of all staff. That incudes, but is not limited to:

- Computers, tablets and other devices
- Access permission for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the 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 their headteacher.

Use of phones and email

Individual schools provides each member of staff with an email address.

This email account should be used for work purposes only.

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 pupils 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 which contains the personal information of another person, they must inform their headteacher immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

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.

Accessing email via your mobile phone

It is accepted business practice that staff will access business emails via their personal phone. However, please be aware that if you lose your phone or it is stolen, unauthorised people may be able to access your work email. If at all possible, protect your phone with a biometric sign in (thumb print or facial recognition) or set up the ability to wipe the phone remotely if you do not have it in your possession. If you are unable to do this, please make sure you advise the Headteacher or School Business Manager if you lose your phone, or have it stolen and work emails can be accessed via the phone. Arrangement will be made to reset your email password to prevent unauthorised access.

Personal use

Staff are permitted to occasionally use Trust/school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/ non break time
- Does not constitute 'unacceptable use'
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

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

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. 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) in line with the Trust/school's policies.

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 pupils and parents could see them.

Staff should take care to follow the Trust/school's guidelines on social media and use of email to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

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

Remote access

We allow staff to access the school's ICT facilities and materials remotely. Access is through Google Drive and we have secure passwords and 2 factor authentication to ensure security of data.

Trust/school social media accounts

The Trust/school has an official social media account e.g. Twitter/Facebook page, managed by headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The Trust/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.

Monitoring of the Trust/school network and use of ICT facilities

The Trust/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 Trust/school monitors ICT use in order to:

- Obtain information related to Trust/school business
- Investigate compliance with Trust/school policies, procedures and standards
- Ensure effective Trust/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

Acceptable Use Pupils

Pupils will be provided with access to the ICT facilities and will be under the supervision of a member of staff.

Search and deletion

Under the Education Act 2011 and in line with the Department for Education's guidance on searching, screening and confiscation, each individual school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under Trust/school rules or legislation.

A Trust 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 Trust/school's rules.

Unacceptable use of ICT and the internet outside of school

The individual school will sanction pupils, in line with their policies, if a pupil 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 Trust/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.
- Activity which defames or disparages the Trust/school, or risks bringing the Trust/school into disrepute

- Sharing confidential information about the Trust/school, other pupils, 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

Learners with Special Educational Needs and Disabilities (SEND)

The internet and technology are an integrated part of everyday life for all children including those with SEND. We understand our responsibilities to keep all children safe online and will implement a range of targeted and differentiated strategies to enable pupils with SEND to access the internet safely and appropriate, adapting the 'acceptable use' rules accordingly.

Acceptable Use Parents

Access to ICT facilities and materials

Parents do not have access to a 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 headteacher's discretion.

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

Communicating with or about the school online

We believe it is important to model for pupils, 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 Acceptable Use Agreement (Pupils).

Data security

The Trust/school takes steps to protect the security of its computing resources, data and user accounts. However, they cannot guarantee security. Staff, pupils, parents and others who use the ICT facilities should use safe computing practices at all times.

Passwords

All users of the Trust/school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

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 pupils 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.

Software updates, firewalls, and anti-virus software
All of the Trust/school's ICT devices that support software updates, security updates, and anti-virus 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 ICT facilities.

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

Data protection
All personal data must be processed and stored in line with data protection regulations and the Trust/school's data protection policy.

Access to facilities and materials
All users of the ICT facilities will have clearly defined access rights to school systems, files and devices. These access rights are managed by the headteacher.

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 headteacher 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.

Encryption
The Trust/school ensures that its devices and systems have an appropriate level of encryption.
Staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the headteacher.

Internet access
The Trust and individual school wireless internet connections are secured.

Use of social media
Each individual Trust school should follow their own policy on the use of social media. However, if you have a concern about what you are seeing or being told to do by another user which has safeguarding implications or may cause harm to the reputation of the Trust/school and/or its community you should contact the headteacher or designated safeguarding lead for advice.

Appendix 1 - Acceptable Use Agreement (Staff)

Acceptable Use Agreement (Staff)

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the designated safeguarding lead, if by a child, or the headteacher, if by another adult in school.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's safeguarding suite of policies on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I understand that I am a role model and will promote positive online safety. I will not engage in any online activity that may compromise my professional responsibilities or bring the Trust into disrepute.
- If the data on any device is breached, I understand it is my responsibility to report it immediately to the appropriate person.
- I will not contact or attempt to contact any pupil or access their contact details in any way other than in school approved methods.
- I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sexting, sharing nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.

The school has a responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policy.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the school's filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in school policies. Where digital personal data is transferred outside the secure local network, I will ensure it is encrypted. Paper based protected and restricted data will be held in lockable storage.
- I understand the Data Protection Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- It is my responsibility to understand and comply with current copyright legislation

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the Academy Council or Trust Board and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

I understand that it is my responsibility to read the schools Online Safety Policy and immediately speak with my headteacher should I have any questions or concerns around the school's online safety arrangements or agreeing to school policies.

Name (staff member/governor/volunteer/visitor): _____

Signature: _____ **Date:** _____

Appendix 2 - Acceptable Use Policy Agreement (Pupil)

Acceptable Use Policy Agreement (Pupil)

Please could parents/carers read and discuss this policy with their child and then sign and return to your child's class teacher.

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

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my password.
- I will only open/delete my own files.
- I will make sure that all online contact with other children and adults is responsible, polite and sensible.
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when online because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my online safety.

Acceptable Use Policy Agreement (Pupil)

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy Agreement.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.
- I will tell a trusted adult in school if anything concerns or upsets me when I am online.

Acceptable Use Policy Agreement (Parent)

- I, with my child, have read and discussed this Acceptable Use Policy (AUP) and understand that the AUP will help keep my child safe online
- I understand that the AUP applies to my child's use of devices and systems on school site and at home and personal use where there are safeguarding and/or behaviour concerns

- I am aware that any use of school devices and systems may be monitored for safety and security reason to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation
- I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to COVID-19. I will ensure my child's access to remote learning is appropriately supervised and in an appropriate location e.g. not in bed and that they are suitably dressed
- I understand that the school will contact me if they have concerns about possible breaches of the AYP or any concerns about my child's safety
- I will inform school or other relevant organisations if I have a concern over my child's or other members of the school community's safety online

Name of Pupil: ……..…. Class: ……..

Signed: ……..…. Date: ……..

Name of Parent: ……

Signed: ……..…. Date: ……..

Name of Parent: ……

Signed: …… Date: ……..

DOCUMENT CONTROL	
Doc Ref:	April 2021
Document Full Title	Acceptable Use Policy
Document Version number	V2
Document stored in	Safeguarding Support Limited
Owned by:	Trust Board
Authorised by:	Trust Board
Date:	July 2021
Review Date:	April 2022
Circulation:	All Staff and Volunteers All Academy Council All Trust Board On Website