Cardinal Hume
Catholic School

ICT Acceptable Use Policy for Students/Parents May 2024

Proud to be part of Bishop Wilkinson Catholic Education Trust

Bishop Wilkinson
Catholic Education Trust

1 Policy Purpose

The purpose of our IT Acceptable Use Policy is to safeguard our students, staff, and the broader school community from inappropriate use, mishandling, or damage of IT resources. These resources provided by Cardinal Hume Catholic School are intended to enhance the educational experience while reflecting our Christian and Catholic values.

As a community, we bear collective responsibility for ensuring that these resources are utilized properly and with integrity. This helps to prevent any actions that could potentially harm the school, its members, or our partners. The school views this policy as a critical cornerstone of our IT management and as such, it is taken very seriously.

Violations of this policy will be addressed according to the school's disciplinary procedures. Severe breaches may be deemed gross misconduct, leading to possible expulsion. This policy should be read in conjunction with the school's disciplinary procedures.

2 Scope

The rules and guidelines set out in this policy apply equally to all employees and students at Cardinal Hume School.

Compliance with the policy is mandatory.

3 Guidelines for Using IT Systems and Communication Devices

a) The IT systems and communication devices provided by Cardinal Hume Catholic School, which include but are not limited to desktop PCs, tablets, printers, and telephones, as well as any other communication platforms currently in use or implemented in the future, must be used responsibly. Inappropriate or unacceptable uses include, but are not limited to:

   i. Accessing, distributing, or engaging in actions that could lead to legal repercussions, damage the school's reputation, or violate the principles of our community. These include:

      1. Sharing explicit content, such as sexually suggestive messages, images, videos, cartoons, or jokes.
      2. Using profane language, slanderous comments, or libellous statements.
      3. Engaging in or promoting ethnic, religious, or racial slurs, or sharing such offensive content.

4. Circulating political, terrorist, or propaganda materials.
5. Harassing or bullying others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs.
6. Promoting illegal substances or criminal activities.
7. Any actions that violate the school's serious misdemeanours policy.

ii. Participating in gambling activities, whether online or via telecommunication devices.

iii. Threatening, harassing, or causing distress, annoyance, or discomfort to any individual or entity.

iv. Circulating inappropriate comments about employees, students, or partners of the school.

v. Misusing IT systems and telecommunication devices in ways that waste resources, disrupt efficient operation of the school's network and systems, or take up unnecessary staff time.

vi. Sending offensive, demeaning, disruptive, or inappropriate messages as determined by the school's leadership. This includes messages that violate the school's equal opportunity and anti-harassment policies. Messages that could be seen as personal, potentially offensive, or frivolous must not be placed on the system.

vii. Sharing sensitive information such as school passwords or account details.

viii. Infringing on others' copyright by downloading, copying, or transmitting their work without permission. Plagiarism, which also infringes on copyright, is strictly forbidden according to the relevant examination rules and procedures.

b) Only school-owned equipment may be connected to the school's network and systems. Personal devices, including but not limited to mobile phones, PDAs, music players, storage devices, local area networks, PCs, and printers, must not be connected without the explicit permission of the school's IT/Network department to ensure the security, reliability, and integrity of the school's IT systems.

c) All users of the school's IT and communication facilities must agree to indemnify Cardinal Hume Catholic School and hold the school harmless from any claims, demands, costs, expenses, losses, and damages arising from their personal use of these facilities.

4 Monitoring and Privacy

a) Cardinal Hume Catholic School reserves the right to monitor and record usage data, including but not limited to internet, email, and telephone usage, as well as the content of emails and internet activity. Monitoring may occur at any time without notice and is conducted in the school's legitimate business interests, such as crime prevention and detection, investigating unauthorized use, virus detection, record keeping, and ensuring compliance with regulations.

b) The school's decision not to monitor certain situations does not waive its right to monitor activities in any or all situations in the future.

c) Personal usage of the school's IT systems and telephones may also be subject to monitoring.

d) As is common practice, emails sent through the school's systems may pass through a gateway between the school's email system and the internet, where they could be subject to additional screening.

e) The school may disclose relevant information to law enforcement agencies to aid in the prevention or detection of crime.

5 Confidentiality and Email Use

a) When using school email accounts, remember that digital communications, including emails, are not as private as you might expect. All email messages are recorded and stored, meaning that even if a message is deleted from a user's inbox, it can often still be retrieved. Given this, refrain from communicating anything through email or over the phone that you would not feel comfortable putting in a written letter. Be aware that digital messages can serve as evidence in legal proceedings.

b) Do not assume that internal messages are private and confidential, even if they are marked as such. Avoid transmitting sensitive or personal matters through email.

c) Treat email messages sent via the internet as non-confidential. As these messages traverse various computer systems with differing security levels, their confidentiality can be compromised at any stage unless encryption is used.

d) School email accounts should not be used to register with external organisations. Use these accounts strictly for school-related communications and activities.

6 Account Security

a) Each student is assigned a unique user account. Use of another's account is strictly forbidden.

b) Respect the boundaries of your account. Attempting to exceed your authorisation level is not permitted.

c) Impersonating another individual on any of Cardinal Hume School's systems or the internet is prohibited. Your name, email address, and related contact information should accurately reflect you as the originator of any message or post.

d) Your password is personal and should not be shared with anyone, except with authorised IT department members for support purposes. If someone might need access to your files in your absence, decide to copy these files to a location they can access.

e) Maintaining the confidentiality of your passwords is your personal responsibility.

f) For password selection, adhere to the following guidelines:

   i. Passwords must be at least eight characters long.

   ii. Passwords should include characters from at least three of the following categories: Upper case letters (A-Z), lower case letters (a-z), numbers (0-9), and special non-alphanumeric characters.

   iii. Your username or any part of your full name should not be part of your password.

   iv. Avoid using the same password you've used previously.

g) Opt for a password that is memorable to you but would be hard for others to guess. It is highly advised against writing down your password.

h) If you suspect that your password may have been compromised, please contact the IT Support Department immediately.

i) To maintain security, you are required to change your password every 60 days. You will receive a warning 14 days before your account is due to be locked. To avoid being locked out of your account, please change your password as soon as you receive this notification.

7 Internet Usage

a) Any connection between the school's network and the internet presents an opportunity for third parties to attempt to access the school's network and the information contained therein. Students must understand that all usage will be controlled and monitored to protect the school.

b) Besides security issues, it's crucial that students use the internet to support their learning rather than for non-educational purposes. Non-school usage of the school's network can adversely affect the performance of critical school systems.
c) Some internet sites are restricted via content filtering. This measure prevents access to inappropriate sites from the school's network. To avoid security breaches or negative effects on the school's network, internet connections from the school's network will only be allowed in accordance with this policy.
d) Students should note that forwarding or storing material that violates this policy may lead to disciplinary actions, including warnings, detentions, or in severe cases, suspension, or expulsion. If you receive such material, you are advised to delete it immediately and contact the school's IT Department.
e) In addition to clause 3 of the policy, other prohibited uses of the internet include, but are not limited to the following:
    i. Downloading, installing, or running software or media files (including pictures, games, music, videos, screensavers, wallpapers, etc.) on any school-owned PC or device attached to the school's network. This includes software for school use, as all software must be approved and tested by the school's IT department.
    ii. Posting information to public discussion groups ("newsgroups"), chat rooms, or other public internet forums on behalf of the school, unless explicitly authorised by a teacher, administrator, or school IT staff.
    iii. Creating any unauthorised web pages, bulletin boards, or other mechanisms that provide public access to information about the school.
    iv. Establishing or using complex data exchange systems (like Electronic Data Interchange), or other electronic business system arrangements.
    v. If you are unsure about whether your internet usage is appropriate or excessive, please discuss this with a teacher, administrator, or member of the school's IT staff.

8 Use of Artificial Intelligence (AI)

a) Artificial Intelligence (AI) tools, including AI chatbots, can generate text, answer questions, analyse and summarise text, author essays and articles, write computer code, translate languages, and more. However, misuse of AI in relation to assessments is considered malpractice.
b) AI tools can provide incorrect or biased information, so students cannot rely solely on their output. Students are responsible for ensuring the work they submit for assessments is their own, reflects their independent work, and is not copied or paraphrased from an AI tool or any other source.

c) AI misuse, defined in the JCQ Suspected Malpractice: Policies and Procedures, includes copying or paraphrasing AI-generated content, using AI to complete assessments, failing to acknowledge the use of AI tools, and submitting work with incomplete or misleading references. Misuse can lead to serious consequences, including disqualification and debarment from taking qualifications.

d) AI tools may only be used under specific conditions: when the assessment permits internet use and the student can demonstrate that the final work product is a result of their independent work and thinking. If AI tools are used as a source of information, students must:

   i. Acknowledge the AI source and date the content was generated (e.g., ChatGPT 3.5, 25/01/2023).

   ii. Retain a copy of the AI-generated content and explain how it was used.

   iii. Submit the above with their work for review by the teacher/assessor.

e) Misuse of AI tools is a serious violation of our academic integrity policy. Be sure to use these tools responsibly and ethically. Seek clarification from your teachers or the IT department if you have any questions or concerns.

9 E-mail Usage and Filtering

a) E-mail is a tool provided primarily for academic use, facilitating efficient communication within the school community. Occasional non-academic use is permitted, but it must adhere to this policy and should not interfere with your schoolwork, consume significant resources, or disrupt the activities of others.

b) School e-mail accounts are professional in nature and should be used for related correspondence. Non-academic or personal matters should be handled through personal e-mail accounts or other suitable channels.

c) E-mails sent from a school account must reflect a professional tone. This means using complete sentences, proper grammar, and maintaining a respectful and courteous demeanour. The content of your e-mails should represent the school well, just as you would when wearing a school I.D.

d) E-mail is not a substitute for other forms of communication such as phone calls or face-to-face conversations, particularly for sensitive topics or emergencies. Learning to discern which mode of communication is most appropriate for a given situation is a crucial part of digital citizenship.

e) Students should be aware that forwarding or storing material that is in violation of the policy can result in disciplinary action. If you receive such material, delete it immediately and report it to your tutor.

f) Unsolicited messages, chain letters, junk e-mail, or spam should not be sent from your school e-mail account. Any alerts or warnings about potential security threats, such as viruses, should be forwarded to the school's IT support department without further action unless instructed otherwise.

g) Offensive or inappropriate material received via e-mail should be deleted immediately and must not be forwarded either within or outside the school community.

h) If you wouldn't say something in public or send it by post, then refrain from sending it via e-mail.

i) Finally, e-mail use should reflect good digital citizenship. This means being conscious and responsible in your online activities, demonstrating respect for others, and avoiding involvement in cyberbullying or other harmful behaviours.

E-mail Filtering

j) E-mail content filters play a crucial role in safeguarding the school from computer viruses, malicious software, and other threats that could damage systems or steal information. They also help prevent overload of the e-mail system with unwanted messages such as advertisements, automated mailshots (often referred to as spam), chain mail, known hoaxes, and scams.

k) Beyond protecting the system's integrity, the content filter also serves to uphold the school's policy and guidelines. E-mails flagged by the content filter are placed in a "quarantine" queue for review. This process ensures a safe and efficient communication environment in line with the school's ICT acceptable use policy.

l) While the filter is designed to catch potentially harmful content, it is important to remember that no system is fool proof. If you encounter suspicious or inappropriate content that has bypassed the filter, delete it immediately and notify your tutor or the IT support department.

m) Remember, e-mail filtering is a tool, not a replacement for good judgement and adherence to our acceptable use policy. Always use your school email account responsibly and consult the guidelines or a member of staff if you are unsure about anything.

10 File Storage

a) All staff and students are required to store their files in OneDrive.

b) Files stored on local hard drives or USB drives are not backed up and may be lost if the device is lost or stolen.

c) OneDrive is accessible from any device with an internet connection and provides 1TB of storage space per user.
d) This is to ensure that all files are backed up and can be accessed from any device with an internet connection.
e) This policy is in place to maintain data security and to allow the personal data of individuals to be protected and deleted after an appropriate timeframe.

11 Legality

a) Ensure that the transmission of personal data outside the school does not infringe the principles of the Data Protection Act (DPA) and the General Data Protection Regulation (GDPR). Personal data is information recorded on a computer or relevant filing system (or recorded with intention that it will go into either), which is biographical, focused and affects privacy. If you have any doubts regarding the transmission of personal data, please contact the SLT member in charge of ICT.
b) Do not use any information, software, or graphics from any published format (books, magazines, brochures and the internet) without obtaining permission from the copyright holder. Any breach of copyright will be taken very seriously.
c) All e-mails sent internally and externally are considered permanent records. Before you send an e-mail, think carefully about its content, and ask yourself how you would feel if you received that message or knew it may be disclosed in court. Your e-mails can be “discovered” in future by outside parties if relevant to court proceedings.

Updated May 2023

Cardinal Hume
Catholic School

Cardinal Hume Catholic School
Old Durham Road Gateshead NE9 6RZ
Tel: 0191 487 7638
Email: info@chs.bwcet.com
www.cardinalhume.com

Proud to be part of Bishop Wilkinson Catholic Education Trust

Bishop Wilkinson
Catholic Education Trust