Acceptable Use Policy

Why have an Acceptable Use Policy?

An Acceptable Use Policy is about ensuring that you, as a student at Carr Hill High School can use the school Network, Internet, Email and other technologies available at the school in a safe and secure way. The policy also extends to other school facilities e.g. desktop, laptop and tablet computers; monitors, projectors and Interactive Whiteboards, printers and peripherals; Internet and Email; Virtual Learning Environments and websites. An Acceptable Use Policy also seeks to ensure that you are not knowingly subject to **identity theft** and therefore fraud. Also that students **avoid cyber bullying** and just as importantly, they **do not become a victim of abuse**.

Help us, to help you, keep safe.

Carr Hill High School recognises the importance of ICT in education and the needs of students to access the computing facilities available within the school. The school aims to make the ICT facilities it has available for students to use for their studies both in and out of lesson times. The school will provide students in Year 7 & 8 with 500 MB of storage, Year 9 with 1 GB of storage, Year 10 & 11 with 2 GB of storage on a school user account and 1 TB of storage on a school Microsoft 365 OneDrive account for educational data. To allow for this Carr Hill High School requires all students to sign a copy of the Acceptable Usage Policy **before** they receive their username and password.

Listed below are the terms of this agreement. All students at Carr Hill High School are expected to use the ICT facilities in accordance with these terms. Violation of terms outlined in this document may lead to loss of access and/or disciplinary action, which will be taken in accordance with the Behaviour Management Policy of the school.

Please read this document carefully and sign and date it to indicate your acceptance of the Policy. Access to the schools network will only take place once this document has been signed by the **BOTH the student and parent/carer.**

1. Equipment

1.1 Vandalism

Vandalism is defined as **any action** that harms or damages any equipment or data that is part of the schools ICT facilities. Such vandalism is covered by the Computer Misuse Act 1990. Vandalism includes, but is not limited to:

- Computer hardware, such as monitors, base units, printers, keyboards, mice or other hardware
- Change or removal of software
- Unauthorised configuration changes
- Creating or uploading computer viruses or malware
- Deliberate deletion of files

Such actions reduce the availability and reliability of computer equipment and put other user's data at risk. In addition, these actions lead to an increase in repairs of the ICT facilities, which impacts upon every student's ability to use the ICT facilities. The other result of vandalism is that it incurs costs, which reduce the funds available to improve the ICT facilities that the school has. Any student caught deliberately vandalising ICT equipment will have the following action taken against them including detention, fixed term or permanent exclusion, and replacement cost recovered from parents/guardians. For serious incidents the full weight of the Computer Misuse Act 1990 will be used.

Carr Hill High School • Royal Avenue • Kirkham • Preston • Lancashire • PR4 2ST
Tel: 01772 682008 Email: contact@carrhill.lancs.sch.uk
www.carrhillschool.com
Headteacher Mr A Waller, MA, BA Hons
Deputy Headteacher Miss A Jordinson, BSc Hons

2. Internet and Email

2.1 Content Filtering

Carr Hill High School provides education specific web filtering with categories fed by The Counter Terrorism Internet Referral unit and Internet Watch Foundation to ensure inappropriate, controversial, offensive or illegal content is removed. However, it is impossible to guarantee that all material is filtered. If you come across any inappropriate website or content whilst using the ICT equipment, **you must report it to a member of staff or IT Services immediately.** The use of Internet and email is a privilege and inappropriate use will result in that privilege being withdrawn. Students can access YouTube in school for educational purposes but this is a filtered version with a strict Safe Search feature to remove inappropriate and explicit videos.

2.2 Acceptable use of the Internet

All Internet access is logged and actively monitored and is stored for up to at least 3 months. Usage reports can and will be provided to any member of staff upon request. Use of the Internet should be in accordance with the following guidelines:

- Only access suitable material – the Internet is not to be used to download, send, print, display or transmit material that would cause offence or break the law.
- Do not attempt to access Internet chat sites, these are blocked and monitored by the school. Remember you could be placing yourself at risk if you do.
- Never give or enter your personal information on a website, especially home addresses, personal telephone numbers, financial details, or usernames and passwords.
- Do not access online gaming sites or download games. Remember that your use of the Internet is for educational purposes only.
- Do not download software from the Internet, as it is considered to be vandalism of the school's ICT facilities.
- Do not use the Internet to order goods or services from online, ecommerce or auction sites.
- Do not subscribe to any newsletter, catalogue or other form of correspondence via the Internet.
- Do not print pages directly from a website. Web pages are often not properly formatted for printing and this may cause a lot of waste. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.
- Do not download pictures, music or videos unless it's for educational purposes and approved by your teacher, copyright permitting.

2.3 Social Networking Websites

The use of social networking websites by students on school computers is prohibited and is blocked by the school. However, the school would remind students that the inappropriate use of social network websites to bully or victimise other students outside of school will impact on them in school as per the schools Behaviour Management Policy. Students and parents are also reminded that the use of these websites outside of school to post derogative material could be inappropriate if it impacts on the school. Parents can get Information about cyber bullying from **www.kidscape.org.uk/cyberbullying**.

2.4 Email

You will be provided with an Email address by the school to be used for legitimate educational and research activity. You are expected to use Email in a responsible manner. The sending or receiving of messages which contain any material that is of a sexist, racist, unethical, illegal or likely to cause offence should not take place. All Email activity is logged and actively monitored against a keyboard alert facility. Any offensive or inappropriate word used in an Email will be automatically flagged and checked. It is recommended that you check your Emails regularly so you do not miss important information and correspondence.

Remember when sending an Email to:

- **Be Polite** and never send or encourage others to send abusive messages.
- **Use appropriate language.** Remember that you are a representative of the school on a global public system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language.
- **Do not reveal any personal information about yourself or anyone else**, especially home addresses, personal telephone numbers, financial details, or usernames and passwords. Remember that Email is not guaranteed to be private.
- **Do not download or open file attachments unless you are certain of both their content and origin**. File attachments may contain viruses that may cause loss of data or damage to the school network.

Last Reviewed: May 2024 Next Reviewed: May 2025

3.0 Privacy and Security

3.1 Passwords

Passwords are an important aspect of network and computer security. A poorly chosen password may result in the compromise of your account or the entire school IT system. All passwords are to be treated as sensitive, confidential school information. Students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords:

- **Never** share your password with anyone else or ask others for their password.
- **Do not** use an account that does not belong to you.
- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be easily guessed, such as your name or address.
- Do not re-use the same password across multiple accounts.
- If you forget your password, inform your teacher and see IT Services for a password reset.
- If you believe that someone else may have discovered your password, change your password as soon as possible (press CTRL + ALT + DEL when logged into a school PC or see IT Services).

Strong passwords:

- Contain upper and lower case characters (e.g., a-z, A-Z).
- Have digits and punctuation characters as well as letters e.g.,0!@#$%^&*()_+|~=\[]:";).
- Are at least six alphanumeric characters long.
- Should not include personal information such as your name.
- A sentence is a good example of a strong password that is easy to remember and hard to guess.

Weak passwords:

- Contain less than six characters.
- Are common usage words such as: names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word, keyboard, or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards or followed by a digit (e.g., secret1).

3.2 Security

- **Never** attempt to access an account, files or programs to which you have not been granted access to. Attempting to bypass security barriers may breach data protection regulations. Such attempts will be considered as hack attacks and will be subject to disciplinary action.
- **Never** use an account other than your own and do not allow others access to your account.
- **Always** ensure you log out of your account when finished using it. You are responsible for all activity that your account is used for.
- You should report any security concerns immediately to a member of staff or IT Services.
- If you are identified as a security risk to the schools ICT facilities you will be denied access to the systems and be subject to disciplinary action.

4.0 Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities and any breach may result in disciplinary action.

- Using the school's ICT facilities to breach intellectual property rights or copyright.
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community.

Last Reviewed: May 2024 Next Reviewed: May 2025

- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Using websites or mechanisms to bypass the school's filtering mechanisms

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

5.0 Mobile Technologies

For safety and security students should not use their smart phone or any other mobile technology in a manner that is likely to bring the school into disrepute or risk the welfare of fellow students. The development of mobile technology is such that smart phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; Mobile Internet access ; Entertainment in the form of video streaming and downloadable video clips from films, sporting events, music, and games, etc. The capabilities of 3G/4G/5G smart phones also means that students within the school environment may be sent inappropriate images or videos, or be encouraged to send back images or video of themselves using integrated cameras. In order to reduce the opportunity for those behaviours that could possibly cause upset it is advisable that students limit their use of mobile technologies in line with the school policy on mobile technologies. If you are sent inappropriate material e.g. messages, images, or videos, etc, report it **immediately to a member of staff** within the school. Chromebooks and laptops provided by the school are classed as mobile technologies. It is prohibited for students to tether their phone to a school laptop or Chromebook to connect to a mobile data connection. Any student caught using a mobile data connection will be disciplined as per the Behaviour Management Policy of the school.

6.0 Printing

All printing is managed by PaperCut software and is chargeable. Year 7 - 11 students are allocated £5 (from April 1st until 31st March each year). To print send your work to the Follow-Me Printer queue. You can then release your printing by entering your PIN at any of the printers located in Art 1st floor, Technology, Main building ground floor (outside the hall), Maths ground floor, The Hub, and outside the Exams office 1st floor.

Printing costs are as follows:

- Single Sided Colour: A3 =4.5p per sheet / A4 = 4p per sheet.
- Single Sided Black & White: A3 = 3p per sheet / A4 = 2p per sheet.
- Double sided Colour: A3 = 1.5p per side / A4 = 1.5p per side.
- Double sided Black & White: A3 = 1.0p per side / A4 = 0.5p per side.

Carr Hill High School • Royal Avenue • Kirkham • Preston • Lancashire • PR4 2ST
Tel: 01772 682008 Email: contact@carrhill.lancs.sch.uk
www.carrhillschool.com
Headteacher Mr A Waller, MA, BA Hons
Deputy Headteacher Miss A Jordinson, BSc Hons

This policy is used in conjunction with the Lancashire County Council Information and Communications Technology ITC Security Framework for schools.

REQUIRED SIGNATURES

STUDENT

I understand and agree to the provisions and conditions of this agreement. I understand that any disobedience to the above provisions will result in disciplinary action and the removal of my privileges to access ICT facilities. I also agree to report any misuse of the system to a staff member and I understand that misuse may come in many forms but may be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal activities, racism, sexism inappropriate language, or any act likely to cause offence.

PRINT NAME _____
SIGNATURE _____
MENTOR GROUP _____
DATE _____

PARENT / GUARDIAN

As the parent or guardian of _____ I have read this agreement and understand that access to electronic information services is designed for educational purposes. I understand that, whilst the Internet service provider operates a filtered service, it is impossible for Carr Hill High School to restrict access to all controversial materials and will not hold the school responsible for materials acquired on the network. I also agree to report any misuse of the system to the school. I hereby give my permission to Carr Hill High School to permit my child access to electronic information services and I certify that the information given on this form is correct.

NAME _____
SIGNATURE _____
DATE _____

Please sign and return IT Services.

Last Reviewed: May 2024 Next Reviewed: May 2025