Staff Acceptable Use Policy

The following statement has been the subject of consultation with the recognised trade unions in Lancashire schools and Lancashire County Council.

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school is keen to see staff make full use of the system, in order that they might broaden their skills and enhance their professional development. The Staff Acceptable Use Policy has been drawn up to protect all parties. With the agreement of the Head teacher, the system and Internet access can be made available for occasional personal use, during the employee's own time i.e. after school and during the lunch break. Staff are reminded that inappropriate use of the Internet could result in action being taken under the terms of the schools disciplinary procedure. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited. Therefore, it is important that all staff familiarise themselves with the principles set out below:

- All Internet activity should be appropriate to staff professional activity, including research for professional purposes. Where the system is made available for personal use, the same principles apply.
- Under the terms of the Authority's Trade Union Facilities Agreement, reasonable use of computer facilities for authorised trade union representatives is permitted.
- Access should only be made via the authorised account and password. Staff passwords should be a complex password containing six characters or more with capitals, numbers or special characters, which should not be made available to any other person; the password policy can be found on the school website and in the Staff Public shared area.
- Activity that threatens the integrity of the school ICT systems and devices, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all Email sent and for contacts made that may result in Email being received; Use for personal or financial gain, gambling, political purposes or advertising is forbidden; Copyright of materials must be respected; Posting anonymous messages and forwarding chain letters or video clips is forbidden; As Email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Use of social network sites, such as Facebook, Twitter and YouTube, are allowed on all school ICT equipment in conjunction with LCC Guidance on the use of social media. You should ensure these are not used is the presence of students, you do not allow students access to these websites via your account, and with the use of YouTube any videos shown to a class are age appropriate.

The Remote Access system allows staff employed at Carr Hill High School to access files and programs installed on the school network. The connection is accessed via a link on the school website. The following guidelines must be observed by all users of the system:

- The Remote Access System is only for use by authorised staff employed by Carr Hill High School. Users must not, under any circumstances, allow other users or unauthorised users to access the system using their login credentials.
- No personal or sensitive data should be accessed or viewed in the presence of any third party or unauthorised user.
- Material uploaded to the network using the Remote Access system must comply with all school guidelines on data storage.
- Users must logoff from the system after use to ensure no connections are left open.

Last Reviewed: May 2021

Next Reviewed: May 2022

Lancashire County Council - ICT Security Policy for Schools

Rules and Agreements for Staff

Rules for ICT Users - Staff

	Notes	Paragraph Reference in ICT Security Policy
1.	Ensure you know who is in charge of the ICT system you use, i.e. the Network Manager.	4.5.1
2.	You must be aware that any infringement of the current legislation relating to the use of ICT systems :- Data Protection Acts 1984 & 1998 Computer Misuse Act 1990 Copyright, Designs and Patents Act 1988 Provisions of this legislation may result in disciplinary, civil and/or criminal action.	5.1.2
3.	ICT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school and as such all users have a personal responsibility for ICT security. Consequently, you must ensure that you receive appropriate training and documentation in the use of your ICT system and in the protection and disclosure of data held.	5.2.2, 6.2, 6.3 & 6.4
4.	Follow the local rules determined by the Head teacher in relation to the use of private equipment and software. All software must be used strictly in accordance the terms of its licence and may only be copied if specifically approved by the Network Manager.	5.4.4 & 8.2.1
5.	Ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. Ensure that equipment is sited so as to avoid environmental risks, e.g. dust, heat. Do not leave your computer logged on, i.e. where data can be directly accessed without password control, when not in attendance. These same rules apply to official equipment used at home.	7.2.1
6.	You must not exceed any access rights to systems or limitations on the use of data granted to you by the Network Manager.	8.4.1
7.	The Network Manager will advise you on the frequency of your password changes. In some cases these will be enforced by the system in use. You should not re-use the same password and make sure it is a minimum of 6 alpha/numeric characters, ideally a mix of upper and lower case text based on a “made up” word, but not obvious or guessable, e.g. surname; date of birth. Do not divulge your password to any person, or use another person's password, unless specifically authorised to do so by the Network Manager, e.g. in cases of shared access. Do not write your password down, unless it is held securely on your person at all times or kept in a locked receptacle/drawer to which only you have access.	8.6.1

Last Reviewed: May 2021

Next Reviewed: May 2022

8.	The Network Manager will advise you on what "backups" you need to make of the data and programs you use and the regularity and security of those backups.	8.7.1
9.	Ensure that newly received CD ROMs and emails have been checked for computer viruses. Any suspected or actual computer virus infection must be reported immediately to the Network Manager.	8.8.1 & 8.8.2
10.	Due regard must be given to the sensitivity of the respective information in disposing of ICT printouts, floppy disks, etc.	8.9.1
11.	Users must exercise extreme vigilance towards any suspicious event relating to ICT use and immediately report any suspected or actual breach of ICT security to the Network Manager or, in exceptional cases, the Head teacher, Chair of Governors or Internal Audit.	9.1
12.	Users of these facilities must complete the declaration attached to the "Acceptable Use Policy".	10.1

E-mail & Internet Use Good Practice

The following guidelines (some of which also apply to other forms of correspondence) tell you what is and what is not good practice when you use internal or Internet Email services.

You should:

- Check your Email inbox for new messages regularly;
- Treat Email as you would a letter, remember they can be forwarded / copied to others;
- Check the message and think how the person may react to it before you send it;
- Make sure you use correct and up to date Email addresses;
- Archive mail when you have dealt with it and delete any items that you do not need to keep;

You should not:

- Use Email to manage staff where face-to-face discussion is more appropriate;
- Create wide-distribution Emails (for example, to addressees throughout the world) unless this form of communication is vital;
- Print out messages you receive unless you need a hard copy;
- Send large file attachments to Emails to many addressees;
- Send an Email that the person who receives it may think is a waste of resources;
- Use jargon, abbreviations or symbols if the person who receives the Email may not understand them.

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

Last Reviewed: May 2021

Next Reviewed: May 2022

REQUIRED SIGNATURES

STAFF AGREEMENT

I have read and understand the Staff Acceptable Use Policy. I will use the computer system, Internet, Email, Remote Access, and other IT systems in a responsible way and obey these rules at all times.

PRINT NAME _____
SIGNATURE _____
DEPARTMENT _____
DATE _____

Please complete, sign and return IT Services.

Last Reviewed: May 2021

Next Reviewed: May 2022