CARBEILE JUNIOR SCHOOL

ACCEPTABLE USE POLICY

Computing Acceptable Use for Staff
Published: October 2013/PH
Reviewed February 2024 MD
To be reviewed: February 2026

General principles
This policy has been drawn up to ensure appropriate levels of:

Availability: ensuring that systems and information are accessible and usable during the school day
Integrity: information is assured with regard to version, accuracy and freedom from corruption
Confidentiality: ensuring information is not disclosed inappropriately
Relevance: ensuring that the school networks, computing equipment, Internet, e-mail and facsimile systems are used in accordance with the business needs of the school.

This Policy has been drawn up in accordance with current statutory provisions relating to information systems including:

Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Criminal Justice and Public Order Act 1994
Data Protection Act 1998
Defamation Act 1996
Disability Discrimination Act 1995
Obscene Publications Act 1959
Race Relations Act 1976
Sex Discrimination Act 1975

Related Documents
E-Safety
Child Protection & Safeguarding
Data Protection
Publication Scheme
Staff Code of Conduct
Confidentiality

Policy Review
We will review this policy bi-annually unless earlier revision is required. All staff will revisit this document bi-annually. Once approved by Governors, the policy will be available to all staff and stored as a hard copy by the Clerk.

Next review: February 2026

Signed Headteacher: Mr P Hamlyn

Signed Chair of Governors:

Signed Computing/ E-Safety Coordinator: Matthew Davey

Date: 2nd February 2024

Computing Acceptable Use Policy for Staff
The use of the latest technology is actively encouraged at Carbeile. With this comes a responsibility to protect users and the school from abuse of the system.
All staff, therefore, must adhere to the policy set out below. This policy covers all computers, laptops and electronic devices (such as iPads, iPod touches and Smart phones) within the school, irrespective of who owns the device.
Staff and pupils are expected to behave responsibly on the school computer network and with the computing equipment.

1) Access
As a staff member at Carbeile, I have access to the following computing facilities:
1.01 Computers throughout the school campus
1.02 Smartboards in teaching rooms
1.03 A secure username and password for logging into school computer systems
1.04 An accredited, filtered Internet connection from any computer in school
1.05 Internal access to the school network to store and share learning resources.
1.06 A personal '@carbeile.cornwall.sch.uk' email account
1.07 Access to network printers.
1.08 Access to resources such as scanners, digital cameras, iPads, visualisers, webcams and microphones.
1.11 Access to the following software for home computer use: Microsoft Office, Smart Notebook 10/11, Adobe, antivirus software
1.12 Access to the School Management Information Systems (SIMS.net) as appropriate to role in school.
1.13 If I bring in my own computing equipment I can see computing support personnel to connect it to the school wireless network.

2) E-safety
2.01 I will ensure that I am aware of e-safety issues affecting staff and pupils. I can visit our e-safety page on the website (www.carbeile.cornwall.sch.uk).
2.02 I will regularly remind pupils of key e-safety messages such as 'never give out personal details online'.
2.03 I will report any accidental access to inappropriate material to my line manager
2.04 I will report any inappropriate websites on CPOMs
2.05 I will be vigilant when asking pupils to search for images
2.06 If a pupil accesses inappropriate material I will report it following the correct procedures
2.07 If I suspect a child protection issue I will report it following the correct procedures.
2.08 I will always be myself and will not pretend to be anyone or anything that I am not on the internet.

3) Computer Security
3.01 I will use computers with care and leave computing equipment as I found it. I will not tamper with computer systems or devices (*eg* printers and projectors) and their cabling
3.02 If I notice that computing equipment or software is damaged or not working correctly, I will report it to the appropriate person straight away
3.03 I will never try to bypass security features or systems in place on the network, or try to access resources or a user account that I do not have permission for (hacking).
3.04 I will never attempt to install software on computers myself and will request a software change through the appropriate person.
3.05 I will always keep my user account credentials secure and not tell them to anyone else.
3.06 I understand that my staff logon gives me access to systems and information that pupils and other staff are not entitled to access and I will not under any circumstances allow anyone else access to a computer under my logon credentials
3.07 I will not attempt to go beyond my authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person or accessing

another person's files. If I find that I do have access to an area that I know I should not have access to, I will inform computing support personnel immediately.
3.08 If I think someone else has obtained my logon details, I will report it to computing support personnel as soon as possible to get my logon credentials changed
3.09 I will never knowingly bring a computer virus, spyware or malware into school.
3.10 If I suspect a school computer or a removable storage device that I am using contains a virus, spyware or other malware, I will report this to computing support personnel.
3.11 I will not attempt to connect to another user's laptop or device while at school. I am not permitted to establish my own computer network
3.12 I will take care if I eat or drink whilst using computing equipment
3.13 I will not reply to spam emails as this will result in more spam. Delete all spam emails.
3.14 If I lose or misplace any portable computing equipment I will inform computing support personnel immediately.
3.15 I will not 'jailbreak' a school iPad, iPhone or iPod touch.

4) Inappropriate Behaviour
4.01 I will not store, download or distribute music, video or image files on my personal user space unless they are copyright free media files related to school work
4.02 I will not send or post defamatory or malicious information about a person or about school
4.03 I will not post or send private information about another person
4.04 I understand that bullying of another person either by email, online or via text message will be treated with the highest severity
4.05 I will not use the internet for gambling
4.06 I will not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people
4.07 If I am planning any activity which might risk breaking the computing Acceptable Use Policy (*eg* research into terrorism for a legitimate project), I will inform the computing coordinator beforehand to gain permission.
4.08 If I mistakenly access material that is profane or obscene, I will inform the Headteacher immediately or I may be held responsible
4.09 I will not attempt to use proxy sites on the internet
4.10 I will not take a photo or video of a pupil or another member of staff who has 'opted out' by notifying the school of their use of images preferences.
4.11 I will not load photos or videos of other staff and pupils to websites or social networking sites. I will refer this job to the Headteacher to ensure that pupils or members of staff have not 'opted out' by notifying the school of their use of images preferences. (*eg* if I wish to put pictures from a trip on the website).

5) Best Practice
5.01 I will not use school printing facilities to print none-work related materials.
5.02 I will only print out work that I need as a paper copy – where possible I will use school systems such as email, the Learning Platform and shared folders to share information electronically for myself and my pupils.
5.03 I will report to the office staff if I believe a printer is not working or out of toner.
5.04 I understand that my @carbeile.cornwall.sch.uk e-mail is a work e-mail account, and as such will be used for professional purposes.
5.05 I will only use the approved, secure @carbeile.cornwall.sch.uk e-mail system for any school communication
5.06 I will only open attachments or download files from trusted sources
5.07 I will not view, download or distribute material that could be considered offensive or pornographic
5.08 I will use a Year Group camera or camcorder to photograph and video trips and relevant events (I will not use my own cameras without prior arrangement).
5.10 I will pass relevant photographs and videos on to the Headteacher to put on the website where relevant. (I will not keep images and videos of pupils in my personal user space and will ensure they are on a shared networking area).

5.11 I will ensure that I regularly back up any work that is not saved onto the school network
5.12 I will observe health and safety guidelines where possible when using computing equipment

7) Data Protection
7.01 I will not share data protected information (including school images) with third party organisations without seeking advice first
7.02 I will use an encrypted storage device to transfer data protected files between home and school.
7.03 If I am preparing a document that contains data protected information I will ensure that the document template I use has the appropriate protective marking (*eg* confidential, protectively marked).
7.04 I will ensure that I am aware of data protection issues and understand what is considered to be 'personal data'.
7.05 I will not display sensitive information or 'personal data' on a public display or projected image (*eg a* smartboard). This includes pupil data in SIMS.net.
7.06 I will never leave a computer logged on and unattended for even a short space of time. I will log off or lock the workstation. I understand that failure to do this may result in a breach of the Data Protection Act and leave 'personal data' unprotected.
7.07 I will ensure that any remote connection session that I have to a school computer is logged off when I have finished and kept secure from other computer users.
7.08 I will use LogMeIn.com appropriately to access the school server from other locations.

8) Social Networking
8.01 I will not communicate with pupils through social networking sites (groups set up due to COVID-19 are exempt from this)
8.02 I will ensure that any personal social networking accounts that I have are secure.
8.03 I will never create a social networking profile or account and use it to broadcast opinions of the school
8.04 If I have control over a school Twitter account I will:

- only follow professional educational organisations
- inform computing support personnel straight away if I suspect I have lost the password or a device with that account on it
- never use the account to send Direct Messages to anyone
- only upload photos of pupils who have the correct permission

8.05 I will never create a bogus social networking account or site that is associated with a member of staff, pupils or the school.
8.06 If I become aware of misuse of Social Networking accounts or sites that are associated with a member of staff, pupils or the school, I will inform the Headteacher immediately.
8.07 I recognise that as an organisation, we do not use social networking sites to communicate with pupils, staff and parents (with the exception of our official Twitter accounts and other during COVID-19)

9) Sanctions
9.01 I understand that failure to comply with this Policy could lead to disciplinary action.