Carrington Infant School
(Carrington Schools Federation)

ICT & Internet Acceptable use Policy
September 2025

MISSION STATEMENT:
The Carrington Schools Federation: an ambitious, caring, and inclusive community.

VISION:
To be a nurturing community that develops respectful, resilient, and happy children with the self-belief, knowledge, and skills to thrive in the future.

Date Policy last reviewed: September 2025
Signed by:
Head Teacher: Kate Cliffe **Date:**
Chair of Governors: Nadia Zachary **Date:**

Overview
This document outlines the network and Internet access policies which the school needs to ensure that the benefits provided by computer systems are not compromised and that pupils, staff and the school are protected from inappropriate use. These policies are based on the Buckinghamshire Council IT policies and should be integrated with the school policies.

Definitions

"ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

"Users": anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

"Personal use": any use or activity not directly related to the users' employment, study or purpose

"Authorised personnel": employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

"Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

Introduction

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.
This policy aims to:

Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors

Establish clear expectations for the way all members of the school community engage with each other online

Support the school's policy on data protection, online safety and safeguarding

Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems

Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary procedures.

User responsibility and behaviour
Everyone is responsible; this could be described as responsible citizenship. All users should expect an acceptable level of ICT service. Similarly, they should expect security

and privacy of their data. This implies mutual respect for other peoples' privacy and data. In public life, to attack other people's accounts, data and personal details might result in job dismissal and possible legal proceedings. Not all school staff realise they are operating in this domain, and together with pupils, need to develop responsible approaches to the use of school ICT facilities.

Pupils will be taught about online safety as part of the curriculum. They will be taught to

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

1. Network Security Policy

Background:
The curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan for and make use of communications technology, for example, web-based resources and e- mail.

Access to life-long learning and employment increasingly requires computers and communications use and pupils need to develop ICT life skills in their use. Home and social Internet use is expanding and it is an important part of learning and communication during leisure time. This brings pupils into contact with a wider range of information, the scope and nature of which may - or may not - be appropriate for the pupil.

Internet Access and Filtering

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Neither the school nor JSL Services Group Ltd can accept liability for the material accessed, or any consequences thereof. The school and JSL Services Group Ltd will undertake to remove unsuitable material immediately if it manifests itself;

- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved;

- Internet access is provided through JSL Services Group Ltd. The service includes filtering appropriate to the age of pupils;

- Pupils use of the Internet will be supervised and monitored whilst at school;

- Security strategies are discussed with JSL Services Group Ltd.

- Filtering of the school's Internet access does not guarantee the safety of pupils and staff, but it is a necessary first step towards protecting our pupils. We appreciate that supervision and education are as important as software solutions.

As we are in contract with JSL Services Group Ltd, they provide Carrington Infant School with an appropriate level of internet traffic filtering.

ICT system integrity and security

The school has a responsibility for ensuring that its capital investment is protected and secured. No users should make changes or modifications to the hardware, network wiring, or software configurations. Only designated support personnel should perform these functions and all work will be logged.

Changes to system or network configuration files and settings are strictly forbidden. Only programmes provided or approved by the school are to be used.
Details of programmes and licences shall be recorded centrally. Anti-virus protection is on all machines connected to the network. Anti-virus strategy is vital to all ICT systems. Site-wide virus screening of systems and external links (email and internet traffic) is essential. All users need to be aware of virus sources and risks.

Risk assessment - considering all possible ICT disaster situations and their consequences is to be part of the school's management policy.

Training and support provision

The school will provide adequate training and support for all users to gain the best use of the ICT resources.

Access to school ICT facilities and materials

The school's business manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

Computers, tablets and other devices

Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's 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 the school business manager.

All access to School systems and data must only be completed via School owned equipment. The use of personal devices is Prohibited.

The use of USB Mass storage devices such as USB sticks or external hard drives is **prohibited** at Carrington Infant School. Any attempt to use these devices will be blocked, logged and reviewed.

The use of External Cloud storage or sharing services is prohibited with the exception of authorised School platforms.
For the avoidance of doubt, you must NOT use any of the following:

- OneDrive personal version
- Google Drive
- Dropbox
- WeTransfer
- Box
- Apple iCloud
- Amazon Drive
- Hightail
- MediaFire
- SugarSync
- Tresorit
- Or any other site or service which is not explicitly allowed.

Explicitly allowed services:
- OneDrive for Business
- SharePoint Online

You must sign into the above services using your @carringtoninf.co.uk account. Any other account sign in or usage is prohibited.

Remote Access

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as required against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Hardware and software quality, maintenance and replacement

All ICT equipment will be recorded on the asset register. Safety testing and maintenance logs will be kept. Hardware maintenance contracts, including network components, hubs and switches, are entered into as appropriate.

Legal duties and responsibilities (licensing, Data Protection and Computer Misuse)
Users should understand that a licence defines software use. Software licences are stored in a secure place. All software shall be used strictly in accordance with its licence. Copying software to and from a network is likely to be illegal. The use of illegal or unlicensed software is an offence. Buckinghamshire Council works with the Federation Against Software Theft (FAST) to ensure software use is legal.

Monitoring of school network and use of ICT facilities

The 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 school monitors ICT use in order to:

Obtain information related to school business

Investigate compliance with school policies, procedures and standards

Ensure effective 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

2. Internet Policy

Carrington Infant School's Internet Service Provider offers the following:

- The facility for multiple access
- Educational content e.g. access to schools' web pages, projects, educational resources, professional discussion groups
- Filtering from the less desirable elements of the internet
- Filtering of junk mail
- Free web space for publishing
- email addresses

Teachers should be familiar with the Pupils' code of practice for use of the Internet and should sign the Teachers' Code of Practice before access to the Internet is provided. Pupils and Parents / Carers should read and sign the Code of Practice for pupils. The Internet, email and web- page creation policies and the codes of practice are available on request.

All users should adhere to the Code of Practice.

The law is quite clear on computer pornography. The Obscene Publications Act 1959 and 1964 make it an offence to publish an obscene article (whether for gain or not) or to have an obscene article for publication or gain (publication includes distribution, circulating, selling, hiring, giving or lending, showing, playing or projecting). The school has a responsibility to control the circulation of obscene materials. Disciplinary action will be taken in the event of staff using the Internet inappropriately.

If pupils either deliberately or accidentally access or download unsuitable materials the school will follow the following procedure:

- The screen will be turned off. Any printed materials or electronic copies will be destroyed.
- Pupil access to the Internet may be suspended.
- Any further action will be in line with the School's behaviour policy e.g. informing parents.
- The Internet Service Provider will be informed.

All Internet activity is to be appropriate to staff professional activity or pupils' education.

The School's Policy on the Internet will be subject to regular monitoring and review in line with the school's policy review cycle.

3. Email policy

The school 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.
For the avoidance of doubt, always encrypt email messages if it contains Personally Identifiable Information (PII) about another individual. This includes, but is not limited to; Full name, email address, date of birth, address, medication or medical conditions, behaviour report, assessment report, identification number and telephone number.

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 the Head Teacher immediately and follow our data breach procedure.

Email shall not be used to create, use, transmit or encourage material which is:

- pornographic, inappropriate or unsuitable
- illegal, obscene or libellous
- offensive or annoying
- defamatory
- in violation of another person's privacy

Personal Use

Staff are permitted to use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. Permission for this may be withdrawn at any time.

Personal use is permitted provided that such use:

Does not take place during teaching hours

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 should NOT use personal computing devices to access School data

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 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.

Personal social media accounts

Staff should take care to protect themselves on social media to avoid compromising their professional integrity. It is advisable that social media accounts are set to private.

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

If a pupil adds you on social media

In the first instance, ignore and delete the request. Block the pupil from viewing your profile

Check your privacy settings, and consider changing your display name or profile picture

If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages.

Notify the senior leadership team or the Head Teacher about what is happening.

If a parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school

Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

Unacceptable Use of ICT

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 the school's ICT facilities includes but is not exclusive to:

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

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

Promoting a private business, unless that business is directly related to the school

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. SLT 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.

Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Head Teacher's discretion upon prior agreement.

How do we recognise a subject access request (SAR)?

An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

All staff members have a responsibility to identify if an individual is making a Subject Access Request and provide the appropriate information.

Any individual should be directed to the School office where the request will be dealt with by a qualified staff member.

4. Pupils' Internet Code of Practice

In order to deliver the National Curriculum it is necessary for the school to give our children access to the Internet. At Carrington Infant School our broadband connection is rigorously filtered by JSL Services Group Ltd – a specialist education broadband provider. The children are always supervised by a member of Staff when using the internet.

- I will only use the internet when supervised by a teacher or adult.
- I will only look at websites my teacher has told me to.

- I will never send anyone anything without permission from my teacher.
- I will only send and receive emails when my teacher has told me to.
- I understand that my emails are monitored by the school network and if I misuse it my parents will be informed.
- I know that my teacher and the Internet Service Provider will check the sites I have visited.
- I will always tell my teacher if anything worries me whilst I am on the internet.
- I will not tell my user name and password to anyone; even my best friend and I will log off my username when I have finished using the computer.
- I may not download software from the Internet (including screen savers, games, video clips, audio clips, *.exe files).

5. Staff, Governors, Volunteers and Visitors Internet Code of Practice

Staff who use the school's ICT are responsible not only for their own actions but also the children under their supervision. It is therefore imperative that staff follow the following code of practice:

Responsibilities for when staff are supervising pupils using the Internet

- Staff shall be familiar with the school's network, Internet, email and web site creation policies and the pupils' code of practice for Internet use.
- Staff shall closely monitor and scrutinise what their pupils are accessing on the Internet including checking the history of pages.
- Computer monitor screens shall be readily visible by the staff, so they can monitor what the pupils are accessing.
- Pupils shall have clear guidelines for the content of email messages, sending and receiving procedures.
- Use of the Internet shall always be supervised by a member of staff.
- Pupils shall be taught skills and techniques to enable efficient and effective use of the Internet.
- The school's Internet Service Provider (ISP) will monitor all web sites visited by the users of the schools ICT. In the unlikely event that offensive materials are found the PC monitor shall be switched off, any printed materials or electronic copies confiscated and offensive URLs shall be given to the ICT Co-ordinator who will report it to the ISP JSL Services Group Ltd.

- Pupils shall have a clearly defined focus for using the Internet and email.
- Virus protection is provided by the school as viruses can be downloaded accidentally from the Internet. Pupils bringing work from home, on any removable media such as a memory stick, could also infect the computer. Any suspicion of a virus within the ICT suite should be reported to the ICT Co-ordinator at the earliest opportunity.
- The ISP will check sites visited by schools.
- Pupils will not use open forums such as chat rooms or social networking such as "Facebook" in this school.
- Staff must be aware that disciplinary action may be taken if, from lack of supervision, pupils are able to use the Internet inappropriately e.g. for accessing pornographic, racist or offensive material for personal financial gain, gambling, political purposes or advertising.
- Pupils should not be permitted to download software from the Internet (including screen savers, games, video clips, audio clips, *.exe files).

Responsibilities for when staff are using the School's ICT for Work Related or Personal Activities

- Staff shall be familiar with the school's network, internet, email and web site creations policies and the pupils' code of practice for Internet use.
- Staff are expected to lead by example and therefore are expected to follow the code of practice set out for pupils.
- Staff are not to attempt to circumvent security measures put in place by the school or Internet Service Provider (ISP).
- Email messages sent externally may be accessed by others. Confidential information should not be sent externally by email without express authority from the Head Teacher.
- Staff should not engage in social networking such as "Facebook" from the school's ICT. If a member of staff chooses to partake in a social network personally then no reference to the school, pupils or other members of staff should be made without the permission of the Head Teacher.
- Staff should not allow visitors or parents to access the school's ICT without permission from the Head Teacher.
- Staff are not allowed to remove ICT equipment from the school without authority from the Head Teacher. When ICT equipment does leave the school premises it must not contain any sensitive or personal information. Staff should be aware that school laptops are not insured by the school in transit between school and home if they

leave your person (e.g. left in the car whilst shopping).
All School ICT equipment that contains personally Identifiable Information must be encrypted

6. Policy on the creation of school web sites

The following protocol for creating web sites shall be followed:

- All links within pages, including links to external sites, shall be fully tested and working and shall be tested to ensure that no unsuitable material can be accessed.
- Any email links shall be cleared with the persons involved and written consent obtained.
- All articles, pictures or icons which are from a "third party" must have copyright clearance in writing.
- Photographs of children whose parents have not given written consent shall not be put on web pages.
- Pages created shall be of high quality without spelling/syntax errors or errors of fact.
- Pages shall link to the home page.
- "Last updated" dates shall be current.
- The school's site shall include a contact and address for the school BUT references to living identifiable individuals are covered by the Data Protection Act and should be avoided.
- Users shall not use the school's website for product advertisement, commercial activities or political campaigning.

7. Online Safety

The following rules will be adhered to following our connection with JSL Services Group Ltd:

- There will be a member of staff responsible for security management
- An Internet Policy will be in place
- An email policy will be in place
- Internet access will be filtered by an approved and current educational solution
- All ICT use will be compatible with the educational objectives of Carrington Infant School

- Pupils' access to programmes will be restricted to Carrington Infant School's pre-loaded software
- Carrington Infant School's Internet Policy will be adhered to when connections are made to external networks
- All installing and downloading of software will be monitored
- Work on classroom computers may require back up from time to time. This will be the responsibility of the Teacher concerned
- There will be access to teacher files as necessary
- To ensure users are aware of their responsibilities, the ICT and Internet Acceptable use Policy will be displayed in the staff room and agreement to comply with the Policy obtained.

Checklist

The school has the following policies in place

Policy on the creation of school website

Safeguarding and child protection (Keeping Children Safe in Education)

Behaviour Regulation and Relationships Policy

Staff code of conduct

Data protection

A parent /carer has seen and signed the Pupils' Code of Practice for the Internet prior to the school providing Internet access.

All staff have read and signed the Teachers' Code of Practice for the use of Internet.