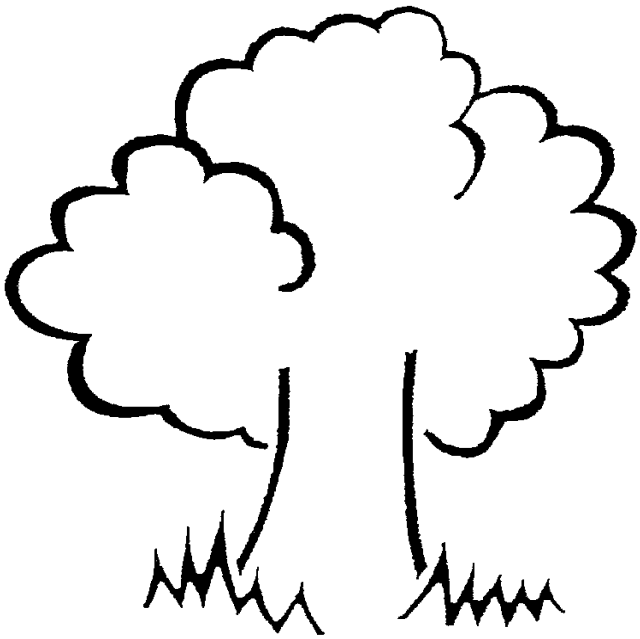
Internet Safety and Acceptable Use Policy

2025

Banks Road Infant and Nursery School



Aims of the policy

Banks Road Infant and Nursery School has a duty to provide children and staff with ICT resources and access to the internet as part of their learning experience. The purpose of ICT use in school is to aid raising educational standards, to promote pupil achievement, to give children work/life skills and to support the professional work staff.

The policy is designed to outline the acceptable use of computers/devices including the use of internet and e-mail. It is a dynamic document in that it will respond to the everchanging ICT environment at the school, as we attempt to stay up to date with ICT advancements to support the National Curriculum. It will therefore be added to and amended as applicable. It is our aim to highlight the 'personal responsibility' of the computer/device user, whether it is for drafting class work on a word processor or using the internet for preparing lessons.

This document sits alongside the school e-safety policy which outlines specific information about our responsibility for keeping safe and how we teach children to manage their digital footprint and stay safe when using the internet.

E-Safety – We aim to teach children how to keep themselves safe so that they are prevented from being exploited and free from extremism. We shall do this by teaching skills and through our values and philosophy of work.

Objectives of the policy

1. Allow staff and pupils the chance to access computer equipment, the internet and email, for educational purposes.
2. Set guidelines for acceptable use of the equipment, hardware and software, so staff and pupils are aware of what is acceptable and not acceptable.
3. Protect pupils and staff from undesirable information, particularly on the world wide web (WWW).
4. Provide rules which are consistent, and in agreement with Nottinghamshire County Council.

Expectations of the ICT User

The following guidelines set Banks Road Infant and Nursery School's expectations for the acceptable use of equipment and use of computers generally around the school by staff and pupils. Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to a member of the senior management Team.

Passwords – passwords are the responsibility of the user and in no circumstances, should they be disclosed in any way. If you suspect somebody knows your password then contact the IT system manager as soon as possible.

Unacceptable files – On a regular basis the IT systems manager will search the network for illegal or unacceptable files; which will in turn be removed.

Network etiquette and Privacy

Users are expected to abide by the rules of network etiquette, these rules include, but are not limited to, the following:

- Be polite – never send or encourage others to send abusive messages.
- Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other group.
- Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other user's files or folders.
- Password – do not reveal your password to anyone. IF you think someone has learned your password then contact ICT Team.
- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
- Users finding machines logged on under another user's user name should log off the machine whether they intend to use it or not.

Hacking - Hacking into or attempting to corrupt the network settings, software or hardware will not be tolerated. Any attempts to do so will be picked up through regular network checks and will be dealt with by a member of the senior leadership team.

Computer damage – Any incidents of damage to the computers (hardware and software) needs to be reported to the IT systems manager immediately; this will then be followed up accordingly.

Use of the internet and e-mail

Banks Road Infant and Nursery School uses a filtered, broadband internet service provider for e-mail and internet access. Pupils and staff will be allowed to use the internet to search for information and resources to meet their professional and learning objectives for information in the school. Pupils and staff will need to be aware that there is no regulatory authority body for the internet, anyone, anywhere can publish materials. It is not censored for opinion, bias or validity of information.

In order to protect sensitive data, staff should use work email accounts, not personal emails when sharing information. Staff must contact parents using office telephone and email account and not their personal devices.

Guidance for school staff regarding social networking sites outside of school

For those who belong to a social networking site (eg Facebook, Twitter, My Space) there are some important issues to note if you want to protect yourself.]

- DO not accept any contact with current of previous pupils
- IF under 18s are on your list be especially careful that content is appropriate including photos.
- Avoid bad language, sexual connotations, obscene jokes
- Avoid criticism of your employer
- Do not post photos of colleagues without their prior permission
- Check privacy settings and do not post comments that may bring your professional status and school into disrepute.
- DO not be friends with the parents/carers of children you have met through your work at Banks Road Infant and Nursery School

Remember that these sites are not always private – often there is a wide access. Ensure that your privacy settings are set to private. Do not say anything that you would not say in public or post comments associated with school which could be easily construed as a breach of confidentiality of even bullying. This is especially important as there have been cases across the country where people have be shown to be showing poor judgement in relation to professional conduct and/or safeguarding which may be recorded on their permanent record which could affect references.

Use of Digital Images

For the purposes of this section publication includes on websites, including social media, in the press, on TV, as web broadcasts or video/CD/CDC to be released into the public domain.

Photography using mobile phones

The use of a mobile phone to take pictures in school is prohibited. If photos were taken using a mobile phone in school an allegation could be made that members of staff have taken inappropriate images with those cameras. Staff are strongly advised to not use the camera within their personally owned mobile phone while on school business. Staff should always use school owned cameras and adhere to the schools policy on photography which outlines where Parental permission is required. If a personal phone is used inadvertently any images must be uploaded to the school network at the earliest opportunity and deleted from the phone with no copies having been kept or transmitted elsewhere and the use reported to the SLT.

School Laptops/Netbooks/iPads/Tablets

Staff should ensure that they have absolute control of a school resource and its use when it is allocated to them. Each member of staff must remember that for a "third party" to use school resources in their home, they would either need to be:

- Logged on by the member of staff personally responsible for the laptop
- Provided with the confidential log in details by the member of staff responsible for the laptop

With this in mind, staff should think about who would be culpable in the unlikely event of an allegation being made.

When persons are viewing material on the internet all people without the assistance of content filters have to make judgements as to whether the content is appropriate or inappropriate. However – inappropriate means different things to different people.

Laptop/Netbook/iPad/Tablet/Learn pad Security

Staff should be aware of the need to preserve the confidentiality of all school information. All personal information is subject to the Data Protection act and should be treated as such.

All staff will be asked to sign a consent form if they are borrowing a school Laptop/Netbook/iPad/Tablet/learnpad (device).

THE POLICY WILL BE REVIEWED ANNUALLY.
DATE OF REVIEW BY GOVERNING BODY: June 2018 June 2019 June 2020 June 2023 June 2024 June 2025 June 2026
This policy was reviewed and ratified by the Pupil and Personnel committee in May 2025. Signed: Chair of Governors_____ Date: _____

Appendix A

Nottinghamshire County Council

Guidance on the Acceptable Use of ICT in Schools

5 May 2025

Guidance on the Acceptable Use of ICT in Schools

ICT learning technologies are an essential resource in Schools today. They help to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Schools need to build in the use of these technologies in order to arm children and young people with the skills to access life-long learning and employment.

Currently children and young people in Schools use these technologies both inside and outside of the classroom for:

- Accessing websites
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality.

Whilst these technologies are exciting and beneficial both in and out of the classroom, all Schools need to be aware of the range of risks associated with the use of these technologies.

To help Schools create a safe ICT learning environment Nottinghamshire County Council (NCC) have produced a guidance document on the acceptable use of ICT in Schools that details the ways in which ICT facilities can and cannot be used by both pupils and staff. The guidance document tries to balance the desirability of fully exploiting the vast educational potential of new technologies whilst providing safeguards against risks and unacceptable material and activities.

Schools should read these documents alongside their ICT policies and implement their own ICT acceptable use policies to ensure all adults and children understand the conditions under which Schools ICT services may be used within their School. Schools have a responsibility at all times to comply with the laws and policies as they relate to the use of ICT facilities whether they are provided by NCC or the School has acquired them through a third party.

If you require further information please do not hesitate to contact ICT Security Architect at NCC on 0115 977 2138 or email: jody.bhoot@nottscc.gov.uk

1. INTRODUCTION

1.1 This guidance applies to the safe use of ICT equipment and services provided by a school. School Governors and head teachers are asked to adopt this guidance and implement it throughout their school.

1.2 Any changes to this guidance will be communicated to schools through the Council's Children and Young People's Services.

1.3 Anyone discovering a breach of this guidance, or who is in receipt of electronic communication that appears to contravene the guidance described below, should raise the issue with the head teacher in the first instance.

2. PURPOSE AND SCOPE

2.1 The purpose of this guidance is to:

- Provide direction and guidance in the use of ICT;
- Encourage consistent and professional practice in the use of ICT;
- Protect School and users from inappropriate usage, security risks and legal liability;
- Ensure that all users are clear about their responsibilities in using ICT;
- Advise users on the monitoring arrangements for the usage of ICT.

2.2 This document applies to:-

- All permanent, temporary and casual staff working at a school;
- Pupils;
- Consultants, contractors, agency staff, governors, parents and others working at the school, including those affiliated with third parties who may be given access to ICT services.

(Note: Throughout this guidance, the word "user" is used to cover all of the above.)

3. TERMS USED WITHIN THIS DOCUMENT

- Appropriate: activities listed are acceptable in terms of ICT use.

- Inappropriate: activities listed as inappropriate may potentially lead to misconduct and disciplinary proceedings. In some cases this could lead to dismissal and legal action.

.

4. PASSWORDS

4.1 The school is responsible for establishing and enforcing a password policy for its use of ICT. The head teacher is responsible for establishing and enforcing a password policy on their systems based on the level of security required. Passwords must be assigned to individual users of ICT systems to maintain security and the data that they contain.

Appropriate:

- Users only using their own account to carry out day to day work;
- Users not disclosing their password to allow others to access their account. Users should be aware passwords are for the benefit of the school and are the proprietary and confidential information of the school;
- Users selecting a password that is easy to remember but not for others to guess;
- Users not selecting obvious passwords, such as the name of a close relative, friend or pet;
- Compliance with the password policy for each computer system.

Inappropriate:

- Requesting passwords personally assigned to other users;
- Using a session via another users password;
- Sharing passwords with other users. All users must take reasonable precautions to protect their passwords;
- If a user thinks that their username or password has been used without their permission, they must change the password and inform the head teacher as soon as practically possible. The head teacher will ensure that new users are issued with appropriate usernames and passwords. When a user leaves their job, whether leaving the school or not, the head teacher will ensure that all usernames and passwords for that user are suspended as appropriate.

5. USE OF E-MAIL AND INTERNET (including Social Media)

5.1 It is the responsibility of a school to ensure that all users use e-mail and Internet service in an acceptable manner and in accordance with the schools acceptable use policy and any e-mail and Internet agreements established by the school. Schools should use Nottinghamshire County Council's email and Internet code of practice for schools to establish their own policies on the acceptable use of email and internet.

5.2 The Internet provides users with access to worldwide information services, bringing new opportunities for communication. With the increasing popularity of social media tools such as Facebook and Twitter thought should be given when using these tools for publishing information about a school.

5.3 Social media tools are excellent tools for teaching and learning and can provide exciting, new opportunities for schools to engage, communicate and collaborate with users and the wider community.

5.4 Whilst social media tools can provide tremendous benefits to schools they also have serious security risks in their use. Risks such as people posting unsafe or inappropriate information about themselves and their personal lives online as well as providing opportunities for offenders to groom and exploit children. In order to mitigate these security risks and still enjoy the benefits of social media schools should establish and enforce good social media usage policies which should include the following points:

- Supervision in the classroom with social media technology must be appropriate to the children's needs and abilities;
- It is good practice for staff to evaluate websites before classroom use. Staff should be aware that websites, search results etc. may be safe and appropriate one day but unsafe a day later. All members of the school community should be aware that filtering software is not always effective and cannot always be relied on alone to safeguard children;
- Children with Special Educational Needs should be appropriately supported according to their specific needs and their personal understanding of the e-Safety risks;
- All pupils and staff should be aware of the school procedure regarding what to do if inappropriate content or messages are found, sent or received online;
- All pupils and staff should understand how to critically evaluate online content;
- Internet filtering must be in place according to the school's requirements. This should be designed with both a technical and curriculum focus and should be agreed by the schools Leadership Team and Governors;
- ICT tools provided by the school should always be used (e.g. work provided digital cameras, memory cards, laptops etc.) rather than personally owned equipment.

6. USE OF PCs, LAPTOPS & SERVERS

Appropriate:

- Storing school data;
- Loading text, images, video or audio streams in connection with day to day work activities;
- Storing limited amounts of personal data (where agreed by the head teacher).

Inappropriate:

- Loading unauthorised or untested software;
- Allowing unauthorised users to access laptops used away from school;
- Failure to keep laptops used away from school secure;
- Storing confidential or personal data or information on removable media without adequate protection or encryption;
- Deliberate, reckless or negligent introduction of viruses;
- Storing personal material protected by copyright which has not been purchased;
- Loading files containing pornographic offensive or obscene material.

7. THE LEGAL FRAMEWORK

7.1 ICT use in a school setting should be legally regulated, this includes the content of e-mail, or sites downloaded from the Internet; privacy issues, monitoring of communications and surveillance at work and employment relations. Further legal advice should be sought, if appropriate, from Council's Children and Young people's Services HR or Legal Services.

7.2 If the school monitors e-mails or scans for profanity/inappropriate content then users should be warned of this through policies.

Appendix B

(Taken from Notts GDPR Toolkit & Framework Document)

Acceptable Personal Use of Resources and Assets Policy

Explaining what is acceptable use of resources and assets provided by us, including IT facilities and covering personal use

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. ***MUST***: You must use our facilities **economically**; your personal use must not create extra costs for us
2. ***MUST NOT***: You must not use our facilities to undertake any unlawful, libellous, immoral or offensive **activities**, including accessing, downloading, storing, creating, copying or disseminating offensive material. This includes, but is not limited to, pornographic, sexual, violent or criminal content and racist, sexist or otherwise discriminatory material
3. ***MUST NOT***: Personal use must not interfere with your **productivity** and how you carry out your duties
4. ***MUST NOT***: Personal use must not reflect adversely on our **reputation**
5. ***MUST NOT***: You must not leave **personal-use websites** open during your working time, even if they are minimised on your screen and you are not actively viewing/ using them
6. ***MUST NOT***: You must not use browsers or access/ attempt to access sites that are knowingly **unacceptable**, even if this is in your own time
7. ***MUST NOT***: You must not **send or forward** chain, joke or spam emails
8. ***MUST NOT***: You must not use the Organisation's facilities for **commercial purposes** not approved by us or for personal financial gain
9. ***MUST NOT***: You must not use your access rights or identity as an employee to **mislead** another person, for personal gain or in any other way which is inconsistent with your role
10. ***MUST NOT***: You must not **disclose** (in writing, speech or electronically) information held by us unless you are authorised to do so, and the recipients are authorised to receive it
11. ***MUST NOT***: When you print, photocopy, scan or fax official-sensitive information, you must not leave the information **unattended**.
12. ***MUST NOT***: You must not **connect** any equipment to our IT network that has not been approved
13. ***MUST NOT***: You must not do anything that would **compromise** the security of the information held by us, such as downloading/ spreading any harmful virus/ program or disabling or changing standard security settings

14. ***MUST NOT***: You must not make personal use of the information available to you that is not available to the **public**

Why must I do it?

1. ALL: To ensure we use our IT and other facilities resources effectively, making sure that our reputation is maintained and to ensure that staff working time is used efficiently on delivering our business outcomes

How must I do it?

1. By checking with your manager or where you have any uncertainty over what is appropriate
2. By complying with the points of this policy
3. You must only make personal use of our IT facilities outside of time you are recording or is designated as your 'working hours'
4. By complying with the points of this policy
5. Closing websites when you are not actively using them
6. By taking care over the sites you are about to open, including reading search report information before opening
7. By deleting such items if you receive them.
8. By checking with your manager where you have any uncertainty over what is appropriate
9. By checking with your manager where you have any uncertainty over what is appropriate
10. If you are not sure if you are authorised to disclose information, speak with your manager in the first instance
11. If you are faxing information outside your immediate office, always make sure that there is someone waiting at the other end to receive it. For other devices, if there is no secure release facility which requires you to be present, you must ensure you wait for the process to complete and remove any originals and copies from the equipment.
12. Check that equipment has been tagged or marked as an accepted and managed device before insertion/ connection.
13. IT controls should prevent your ability to download anything harmful, but if in doubt, contact your manager in the first instance.
14. If you wish to utilise Organisation data in a personal capacity, you must make a formal request for information to the Organisation.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

BANKS ROAD INFANT AND NURSERY SCHOOL

"A Home for Learning, Laughing, Caring and Trying"

Document Control

Version:	1
Date approved:	22.05.2025
Approved by:	Governing Board
Next review:	June 2026

References

- Data Protection Act 2018
- General Data Protection Regulations 2016

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.