



Nottinghamshire County Council

Guidance on the Acceptable Use of ICT in Schools and Mobile Phone/Camera Policy

2

This policy was adopted: October, 2020.

This policy was last reviewed: October, 2025.

Source: Nottinghamshire County Council Model
Policy September 2019.

Contents

1. Introduction	Page 3
2. Purpose and scope	Page 4
3. Terms used within this document	Page 4
4. Passwords	Page 4
5. Use of e-mail and internet (including social media)	Page 5
6. Use of PCs, laptops and servers	Page 6
7. The legal framework	Page 6
8. Mobile phones	Page 7
9. Procedures	Page 7
10. Learning Journeys	Page 8
11. Use of a Professional Photographer	Page 9
Appendix 1 – Children’s records/learning journey/profiles consent form	Page 10
Appendix 2 – Additional consent to use an image form	Page 11

Our School Vision

Our school vision is based on the theme of '*Taking Care*'. We strive to encourage our children, staff and wider community to 'take care' of one another through the core Christian Values of:

Kindness, Hope, Courage and Respect.

Our vision is inspired by the words in Corinthians:

"Let love and kindness be the motivation behind all that you do."

(1 Corinthians 16.14)

Ravenshead C of E Primary School is committed to valuing diversity and to equality of opportunity.

In biblical tradition, children in particular are seen to hold a special place in the priorities of God. Furthermore, we hold to the foundational belief that all people are created in God's image and are intrinsically valuable. Everyone should be treated as fundamentally precious, irrespective of behaviour, achievements or potential.

Therefore, we aim to create and promote an environment in which pupils, parents/carers and staff are treated fairly and with respect and feel able to contribute to the best of their abilities. The school's biblical foundation provides a model of Christian community described as the 'body of Christ', in which everyone has a part to play, and everyone without exception has God-given gifts which are to be used for the benefit of others.

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 and Families Department.
- 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.
- 1.4 This policy incorporates the statutory requirements in relation to the Early Years mobile phone and camera usage.

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 user's 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 Headteacher).

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 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.

8 MOBILE PHONES

8.1 Staff are allowed to bring their personal mobile phone to school. Practitioners must ensure that there are no inappropriate or illegal content on their device.

8.2 All staff must ensure that their mobile phones are left inside their bags.

- 8.3 Mobile phone calls can be taken in the staffroom at break times.
- 8.4 If a personal emergency should occur, staff are allowed to take their mobile phone into the classroom. They must first seek permission from the Headteacher, Deputy Head or Assistant Head.
- 8.5 The school hold details of each practitioner's emergency contact number of the next of kin.
- 8.6 All helpers will be requested to leave their mobile phone in their bags.
- 8.7 The school mobile phone will be taken on trips/visits for emergency purposes. It is the responsibility of all members of staff to remain vigilant and report any concerns to the Headteacher.
- 8.8 KS2 children are allowed to bring their mobile phones to school but these must be handed into the Main Reception first thing in the morning and collected at the end of the day (they are locked in a filing cabinet with only office staff having access). *Ravenshead C of E Primary does not accept any responsibility for loss or damage to mobile phones brought to school by the children.*
- 8.9 Mobile phones **must not** be used to photograph children. The school iPad can be used to photograph children and all classes have access to one of these.
- 8.10 The Headteacher or Deputy Head reserve the right to check the image content of a member of staff's mobile phone should there be any cause for concern.
- 8.11 Should inappropriate material be found the Local Authority Designated Safeguarding Officer (LADO) will be contacted immediately. Appropriate procedures will then follow (please refer to the Staff Code of Conduct and Disciplinary Procedures for further details).

9. PROCEDURES

- 9.1 Consent is required under the Data Protection Act 2018 and GDPR guidelines as images are considered to be personal data.
- 9.2 All images are to be stored and disposed of in line with Data Protection Act 2018 and GDPR regulations.
- 9.3 Security procedures must be monitored and reviewed regularly by the designated safeguarding officer. The security procedures include protection against theft of equipment and computer security.

- 9.4 **Consent forms must be signed by parents/carers with parental responsibility when they register their child with the setting.**
- 9.5 Images must not be used for anything other than the agreed purposes agreed by parents unless additional consent is obtained.
- 9.6 Photographs must be appropriately disposed of should they be no longer required. This could include giving the images to parents, deleting or shredding.
- 9.7 Where group photographs of children are to be taken, permission must be obtained from all parents /carers who have the right to refuse.
- 9.8 The purpose and context for any proposed images should always be considered to decide whether a photograph or video are the most appropriate method of recording the information.
- 9.9 The purpose of taking any images is to be clearly explained for example marketing of the business, prospectus, website, or local newspaper, use in display and to document children's learning.
- 9.10 Each reason is to be clearly explained and agreed with an option for parents/carers to refuse any or all of the discussed uses and to withdraw consent at any time. Consents are asked for each year via the Arbor parent app.
- 9.11 Consent for the use of images applies to adults as well as children.
- 9.12 A child's full name should not appear alongside their photographs if the images could be viewed by the general public.

10. LEARNING JOURNEYS

- 10:1 Learning journeys are to be treated as personal data as each journey relates to an individual, identifiable child. Class Dojo is used for Y1-6 and Seesaw for F1 and F2.
- 10.2 Where possible, blanket consent will be requested from parent and carers for group images to be included in the learning journeys of other children. Parents and carers must be given the opportunity to view any images before they are included in any learning journey and must be given the option to restrict their consent.
- 10.3 If it is not possible to obtain consent, the relevant image must not be shared across learning journeys of other children.

- 10.4 Parents and carers must be reminded that they must not share, distribute or display images containing other children without the relevant permission or consent from their parents/carers.
- 10.5 Parents should be encouraged to contribute information to this learning journey, by including some information and photographs which show what their child enjoys doing at home.
- 10.6 Learning journeys should remain on site at all times. If learning journeys are taken off site, this must be with prior agreement between headteacher/practitioner and parents and a risk assessment should be undertaken.

11. USE OF A PROFESSIONAL PHOTOGRAPHER

- 11.1 Only a reputable photographer who can provide evidence of authenticity should be used. Their photographic identity should be checked on arrival.
- 11.2 They should be viewed as visitors therefore appropriate supervision should be in place at all times to ensure no unsupervised access to children. They should be supervised by a person who is in regulated activity.
- 11.3 They should be asked to sign an agreement to ensure that they comply with Data Protection requirements, to agree that images will only be used for the agreed specified purpose and not be disclosed to any third person.

12. Links to other policies

- Child Protection Policy.
- Online Safety Policy.
- Staff Code of Conduct.
- Disciplinary Procedures.
- Class Dojo Policy.
- Peer on Peer Abuse (Child on Child) Policy.

APPENDIX 1

Children's Records/Learning Journey/Profiles Consent Form

To *(Name of parent or carer)*

Re: *(Name of child)*

As encouraged throughout the Early Years Foundation Stage, we will have in place detailed individual learning journeys for all children in our setting, which will document, evidence and monitor their learning and development progress.

In all children's learning journeys, we will include observations of your child at play, photographs and other information. The photographs could include individual and group play. It is likely that some of these group photographs will capture other children at play, so we therefore ask that you give permission for any photographs of your child involved in group play to be included in other children's learning journeys.

Please note that you will be given the option to view any photographs before they are included in any learning journey, should you request this.

As a parent/carers you will also be able to restrict your consent to only allow group photographs (which picture your child) to be included in specific learning journeys. If you would like to restrict your consent to specific learning journeys please state this in writing and return with this consent form.

Please also note that should any parent/carers not grant consent to include group images in other learning journeys, relevant images will not be shared across the learning journeys of other children.

If permission is granted for the sharing of images across learning journeys, these images cannot be shared with others or publicised in any way without the explicit consent of the parents /carers whose children may be included i.e. any social networking site.

This form is valid for the duration of your child's time at our early years setting.

The consent will automatically expire after this time. It is your responsibility to let us know if you want to withdraw or change your consent at any time.

I consent /do not consent to group photographs being included in other children's learning journeys
I understand that any data included in my child's learning journey which relates to another child is for my information only and I will not be publicise or share it in any way.

Signature of parent/carers:

Name:

Date:

APPENDIX 2 Additional Consent to Use an Image Form

Dear (*name of parent/carer*)

We would like to use a photograph of your child for the following purpose: (*list purpose*):

The period of time this image would be used is from..... to.....

After this time, the photograph will be returned to you or destroyed.

We will not share the photograph with any third party or use the image for anything other than the agreed purpose.

Consent:

I have read the above statements, and **I agree / do not agree** to this image being used.

Signature of parent/carer:

Print Name:

Name of Child:

Date:

A copy of the photograph referred to in this consent form is attached.