Nottinghamshire County Council

Guidance on the Acceptable Use of ICT in Schools

27 September 2017

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.