Millbrook Primary School

Use of ICT Systems

July 2019

Table of Contents

1. Definitions

ICT: Information and Communications Technology, typically Computing/Computer systems, consisting of elements of hardware, software and peripheral equipment designed to facilitate the processing of information by electronic means and communication technologies including hardware and software designed to facilitate communication between a group of computers (a wired or wireless network) and between individuals (wired and wireless telephony). For the purposes of this document, ICT and Computing are interchangeable terms and mean the same thing.

The policy: throughout this document, references to 'the policy' shall refer to this document.

The school: The school is Millbrook Primary School, Worsley Road, Freshbrook, Swindon, SN5 8NU. A company limited by guarantee and registered in England and Wales with the company registration number 08713217.

Confidentiality, Integrity and Availability (CIA): The three tenets of an Information Security Policy address are the confidentiality – how private information is kept private; integrity – how an organisation can ensure that information is correct and has not been tampered with and Availability – how an organisation can ensure that the right information is available and accessible to the right people at the right time.

2. Introduction

The use of ICT is a prerequisite to living in the modern world. It enables rapid and effective processing of information and facilitates simple and effective communication between individuals. It's use however is not entirely risk free: confidentiality, integrity and availability of information can be jeopardised if checks and balances are not put in place to ensure such use is authorised, appropriate and safe. This policy outlines the standards to which all individuals must adhere when using the school ICT systems; the circumstances under which the school will monitor their use, and the action which will be taken in respect of any breaches of these standards.

3. Scope

This policy outlines the responsibilities of all members of staff, contractors, governors, volunteers, pupils and visitors to the school who are granted, for whatever reason and for whatever duration, access to the ICT systems at the school.

A breach of this policy may be considered a disciplinary offence and will be dealt with accordingly.

4. Roles and Responsibilities?

4.1. The Governing Body

The governing body of The School will:

- own and manage the policy throughout its lifetime
- periodically review the policy and consider its ongoing relevance
- ratify and suggest reasonable amendments, including best-practice, to the policy

4.2. The Head Teacher

The head teacher will:

- develop and maintain the policy on behalf of the governing body
- take the lead role in investigating any alleged breaches of the policy and, where necessary, apply sanctions as required
- appoint or outsource sufficient technical ICT support services as required

4.3. Appointed/Outsourced ICT support

The appointed/out-sourced ICT support provider will:

- ensure, as so far as is reasonably practicable within their restrictions of their contract, that the school has the most useful and secure ICT systems possible
- configure the ICT systems to ensure the CIA of the information and systems at all times
- prioritise any support requirement that may have an impact on the security of the system or the information processed upon it
- keep the head teacher apprised of the condition of the ICT systems
- alert the head teacher to any suspected misuse of the system or breach of security

4.4. Users of The School's ICT

All users of The School's ICT systems will:

- familiarise themselves with the contents of this policy
- report any suspected breaches of the policy to the head teacher. If the breach is likely to be considered to jeopardise safeguarding, the procedures documented in the safeguarding policy should take precedence.
- raise, at the earliest opportunity, any support/software requirement with the appointed ICT support provider

5. Guarding against unauthorised use

All users have a responsibility to ensure the **confidentiality**, **integrity** and **availability** of information processed by the school's ICT systems and must:

- not allow any ICT systems to be used by anyone other than in accordance with this policy
- ensure all devices are left locked or logged off, to prevent unauthorised users accessing the system, when leaving them unattended
- ensure all mobile ICT equipment is kept physically secure when taking it off the premises. This is especially important when transporting it by car, where it must remain out of sight and preferably locked in the boot

6. Password security

All users must:

- ensure all passwords are kept confidential and not shared with anyone else
- change passwords regularly when prompted by the system to do so
- avoid moving or tampering with equipment to prevent unnecessary damage

7. Network security

Users must not:

- share the wireless network encryption key (password) with anyone not entitled to use it
- connected any issued device to any untrusted third party network when working off-site.

8. System security

Users must not:

- delete or modify any installed software without approval from the computing coordinator or appointed ICT support engineer

- download or install any third party software without prior approval, ensuring that the software is obtained from a trusted source and appropriately licensed for commercial use

9. Use of the World Wide Web

The school employs a web filtering system on the upstream Internet connection to prevent access to content which may harm the children and security of the ICT system. Users must:

- not attempt to access any material which may be considered harmful, illegal, offensive, immoral or in bad taste
- not attempt to circumvent the installed network filtering systems by any means
- have due regard to the Use of Social Media policy when accessing social media platforms
- alert the head teacher, computing coordinator or ICT support engineer in the event that the filtering system permits access to something they consider inappropriate for it to do so

10. Use of E-Mail

All staff and governors are issued with a school e-mail address. Staff and governors must:

- conduct themselves with integrity and in accordance with accepted professional standards when communicating by e-mail, especially to third parties. E-mail is not to be used to share gossip, jokes or content not appropriate for the workplace, even if it is individual to individual.
- remember that all e-mails are subject to the data protection act and freedom of information act and may be requested by individuals making subject access requests or freedom of information requests
- never assume the sender address is genuine and confirm verbally before performing unexpected actions, especially clicking on web links, opening attachments or replying with information
- not use e-mail to share content in breach of copyright including downloaded images, music, video or text

- ensure e-mails are kept concise, correctly spelt and informative. Keep formality and courtesy levels high until the relationship between the recipients dictates otherwise
- consider the correct use of To, CC and BCC fields. E-Mail addresses are personal information under the data protection act and must not be shared without consent. Mailshots to multiple recipients should use the BCC field unless all recipients know each other
- ensure attachments are readable by all recipients (i.e. they are using compatible software) and are not excessive in size
- Only use reply-all when all recipients of the original e-mail need to know your response

11. Personal Use of Systems

Limited personal use of systems is permitted providing such use is accordance with this policy and does not impact their professional duties.

Users are reminded that all access to the system is subject to monitoring and may be recorded for lawful purposes. Use of issued assets for personal use, by the individual to which they have been assigned, at home is permitted but discouraged. Use by the individual's family members would be considered unauthorised use and is not permitted.

12. Systems Monitoring

The school will use all available means of monitoring access and use of the ICT systems including the photocopier to ensure appropriate and professional use. The system is unable to distinguish between professional and personal use, so users are advised to avoid personal use if they do not wish it to be captured/logged.

Reports on usage are provided to the head teacher from time to time upon request.

13. Document Control

Document Title:	Use of ICT Systems
Document last reviewed:	7/23/2019
Next review due:	2 Years