LONG SUTTON PRIMARY SCHOOL

ICT Acceptable Use Policy

Document Control

Date	January 2019
Version Number	V1.0
Author	
Approved by	

Contents

1. Aim

The aim of this policy is to set out individual responsibilities which assist Long Sutton Primary School (the school) in protecting its Information and Communication Technology (ICT).

It supports the school's Information Security Policy.

2. Scope

The policy applies to:

- Any individual using or accessing school ICT;
- School owned or leased ICT such as PC's; laptops; notebooks; smart phones; software; services, storage media and network resources.

3. Training and Awareness

You must undertake information security and data protection training on a regular basis.

4. General Responsibilities

You must protect your user name, password, and security token (if used) against misuse.

All ICT must be subject to access control to ensure only authorised persons can access the ICT.

You must operate a clear screen policy when you leave your device unattended e.g. locking your computer by pressing the Windows key and the 'L' key simultaneously or by engaging the lock screen on your smartphone.

You must protect portable devices and removable media at all times. When not in use they must be subject to appropriate security e.g. placed out of sight under lock and key.

You must ensure all portable ICT used to store or process sensitive information, such as personal data, is encrypted.

You must ensure all ICT is returned to [insert contact] when no longer required. This is to ensure devices are securely wiped or destroyed.

You must only access or attempt to access ICT that you have been authorised to access.

You must only access or attempt to access information for official school purposes aligned with your role and this must be on a need to know basis.

5. Unacceptable Use

You must not use the username and password of another person or share your own username and password with another person.

You must not misuse, bypass or change the configuration or security settings of any ICT.

You must not introduce unauthorised software, hardware, or removable media.

You must not process or access racist, sexist, defamatory, offensive, obscene, illegal or otherwise inappropriate material.

You must not carry out illegal, fraudulent or malicious activity.

You must not use school ICT to carry out or support business which is unrelated to the school.

You must not break copyright or carryout any activity that negatively impacts intellectual property rights.

6. Internet Use

Use of the Internet is encouraged where such use supports the school's objectives.

You must not use the Internet to visit websites or post comments, remarks or any other material that could be construed as racist, sexist, defamatory, offensive, obscene, illegal or otherwise inappropriate.

If you access inappropriate material by accident you must advise [insert contact]

You must not download electronic files or software without authority from [insert contact].

You must not use the Internet to illegally share, reuse, or copy materials which are copyrighted and/or licensed.

Personal use of the Internet must be reasonable, proportionate and occasional.

7. Email

You must only send emails from your own authorised account.

You must check that the recipients of e-mail are correct to avoid accidental release to unintended recipients. Particular care must be taken when using auto complete in your email client as an unintended email address may be used in error.

You must not use personally owned email accounts to conduct school business or to transmit or receive school information.

You must take care when opening an attachment or clicking on any link within any email unless you are confident the email is legitimate.

Suspicious email should be deleted and must not be forwarded to other recipients.

If you suspect an email contains malware please contact [insert contact].

When sending an email to more than one recipient and it is necessary to protect email addresses the blind carbon copy (BCC) feature must be used.

When sending sensitive information via email you must ensure it is done so securely. [Insert how you normally achieve this].

Personal use of school email shall be reasonable, proportionate and occasional and must not interfere with the performance of your role or the performance of the system.

Delegate access to email accounts must only be provided following a clear business need and only when authority is provided by the email account owner, or in their absence, the Head Teacher. To arrange delegate access please contact [insert contact].

Delegate access must not be provided by supplying details of a User's credentials i.e. username and password.

When provided with delegate access the person accessing emails must take reasonable precautions to avoid opening private emails. If it becomes readily apparent that an email is of a personal nature the reader must not open it or stop immediately if the email has been opened.

8. Passwords

Passwords must not be shared and must be protected from unauthorised disclosure.

When creating a passwords ensure it is not easily guessable e.g. ‘letmein123’, 'Password1' and avoid using keyboard patterns or sequential numbers e.g. qwerty, 12345.

Passwords must be [X] characters in length.

Passwords must not be recorded unless it is done so securely and you are the only one who can access is it.

The same password must not be used across different accounts (work and private) and/or applications.

Default passwords must be changed.

9. Removable Media

Removable media which contains sensitive information such as personal data must be encrypted. Removable media includes USB flash drives, CDR, DVDR, removable hard drives.

Removable media from an unknown source must not be introduced to school ICT as it may contain malware designed to harm school systems.

10. Remote/Mobile Working

Additional care must be taken when working outside of school premises and you must ensure that reasonable safeguards are taken to manage the increased likelihood of a security incident.

You must only remove ICT from school premises when there is a clear business need.

You must prevent inadvertent disclosure of information and avoid being overlooked when working.

When removing ICT from school premises, and it contains sensitive information such as personal data, only do so if it is encrypted.

You must avoid storing ICT in an unoccupied vehicle unless more secure options are unavailable. If it is unavoidable then you must place the ICT out of sight, in the locked boot of the vehicle.

ICT must never be stored in a vehicle overnight.

Portable devices must connect to the school's ICT network on at least a monthly basis in order to receive security updates. You must ensure devices remain connected until such time updates have been received and applied i.e. Windows updates.

11. Reporting Security Incidents

All security incidents and suspected security incidents must be reported in accordance with the school's Security Incident Policy.

If you identify suspicious activity while using ICT or believe that you are the victim of malware e.g. a virus you must stop what you are doing, power off your ICT and report it immediately.

You must report all security incidents to [insert contact].

12. Monitoring

The school reserves the right to monitor its communication systems and services.

This includes, but is not limited to, email, telephone conversations, electronic messaging, internet use, and system access.

Monitoring is used by the school for the following purposes:

- To maintain and ensure security of systems and information;
- To check for unauthorised use;
- To establish facts relevant to school business;
- To ensure quality assurance and ensure that procedures are being followed;
- To undertake disciplinary, performance, and capability proceedings; and
- To prevent or detect crime.

13. Further Information

For further information regarding ICT acceptable use within the school please contact:

Tracey Roscher
School Business Manager
tracey.roscher@longsutton.lincs.sch.uk
01406 363381

Joe Lee (ARK IT Services)
Data Protection Officer
[insert email address]
[insert phone number]

Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk.

14. Review

This policy shall be reviewed annually.