Winchelsea

All Individuals Matter

WINCHELSEA PRIMARY SCHOOL
RUSKINGTON

ACCEPTABLE I.C.T. USE POLICY

ALL ADULTS AT WINCHELSEA

June 2024

Aims

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

The policy applies to:

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

Training and Awareness

Staff should undertake relevant information security and data protection training on a regular basis.

General Responsibilities

- Staff must protect their usernames, passwords and any other security details e.g. security tokens (if used) against misuse. All ICT must be subject to access control to ensure only authorised persons can access the ICT.
- Staff must operate a clear screen policy when leaving devices unattended e.g. locking a computer by pressing the Windows key and the 'L' key simultaneously or by engaging the lock screen on a smartphone.
- Staff 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.
- Staff must ensure all portable ICT used to store or process sensitive information, such as personal data, is encrypted.
- Staff must ensure all ICT is returned to the Business Manager when no longer required. This is to ensure devices are securely wiped or destroyed.
- Staff must only access or attempt to access ICT that they have been authorised to access.
- Staff must only access or attempt to access information for official school purposes aligned with their role and this should be on a need-to-know basis.

Unacceptable Use

- Staff must not use the username and password of another person or share their own username and password with another person.
- Staff must not misuse, bypass or change the configuration or security settings of any ICT.
- Staff must not introduce unauthorised software, hardware, or removable media.
- Staff must not process or access racist, sexist, defamatory, offensive, obscene, illegal or otherwise inappropriate material.

- Staff must not carry out illegal, fraudulent or malicious activity.
- Staff must not use school ICT to carry out or support business which is unrelated to the school.
- Staff must not break copyright or carry out any activity that negatively impacts intellectual property rights.

Internet Use

- Use of the Internet is encouraged where such use supports the school's objectives. Staff 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 staff access inappropriate material by accident they must advise the Head teacher immediately.
- Staff must not download electronic files or software without authority from the Head teacher.
- Staff 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.

Email

- Staff must only send emails from their own authorised account.
- Staff must check that the recipients of emails are correct to avoid accidental release to unintended recipients.
- Staff must not use personally owned email accounts to conduct school business or to transmit or receive school information.
- Staff must take care when opening an attachment or clicking on any link within any email and only when confident the email is legitimate. Suspicious emails should be deleted and must not be forwarded to other recipients.
- If staff suspect an email contains malware, they should contact the school's ICT Technician at Ark ICT Solutions Ltd or the Ark Support Team.
- 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 staff must ensure it is done so securely. To achieve this type EncryptMail in the subject box prior to any text when composing an email. This will ensure that the email is sent securely.

- Delegating 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 the Ark Support Team. Delegate access must not be provided by supplying details of a user's credential 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.

Passwords

- Passwords must not be shared and must be protected from unauthorised disclosure. When creating a password staff should ensure it is not easily guessable e.g. "letmein123", "Password1" and avoid using keyboard patterns or sequential numbers e.g. qwerty, 12345. Password length is dependent on the individual system being used. When setting, staff should check the on-screen guidance. Passwords must not be recorded unless done so securely. The same password must not be used across different accounts (work and private) and/or applications. Default passwords must be changed.

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.

Remote/Mobile Working

- Additional care must be taken when working outside of school premises and staff must ensure that reasonable safeguards are taken to manage the increased likelihood of a security incident.
- Staff should only remove ICT from school premises when there is a clear business need.

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

- When removing ICT from school premises that contains sensitive information such as personal data it must be encrypted.

- Staff must avoid storing ICT in an unoccupied vehicle unless more secure options are unavailable. If it is unavoidable then staff 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. Staff must ensure devices remain connected until such time updates have been received and applied i.e. Windows updates.

Reporting Security Incidents

- All security incidents and suspected security incidents must be reported in accordance with the school's identified procedures.

- If a staff member should identify suspicious activity while using ICT or believe they are the victim of malware e.g. a virus, they must stop what they are doing, power off their ICT and report it immediately.

- All security incidents should be reported to ARK.

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.

Signed: _____ Dated: _____
Chair of Governors