SOFTWARE

- All software should comply with relevant guidelines issues by IT Services.
- All requests for software must be sent to IT Services who will arrange for its procurement and installation.
- Only software that has been purchased and/or authorised by IT Services should be used within Whinney Banks Primary School and/or on Whinney Banks Primary School equipment.
- The use of unauthorised software on Whinney Banks Primary School equipment is strictly prohibited. Usage of such software may result in the introduction of viruses or similar malevolent software and may compromise the integrity of Whinney Banks Primary School's computing environment. Furthermore, unauthorised software may result in fines and/or other associated penalties to the individual user and Whinney Banks Primary School.

ELECTRONIC MEDIA

All media used to store information or data should utilise any in-built security features and should be securely stored at all times when not in use.

IT CHANGES

Changes to Whinney Banks Primary School's operational environments must be performed in a controlled manner. Inadequate control over changes is a common source of system downtime and/or security failure. Therefore, assessment of proposed changes (or introductions) must be performed in order to assess the potential impact to Whinney Banks Primary School's computing environment. All changes should be performed in accordance with Whinney Banks Primary Schools Change Control procedures.

IT SERVICE DESK

Problems encountered when using Whinney Banks Primary School's IT systems should be reported to and logged by the IT Helpdesk. This ensures that problems are managed effectively and that they are prioritised and resolved in a timely manner.

PRINTED OUTPUT

All printed output containing sensitive information should be controlled and only available to authorised personnel. All printed documents should be collected and printers, faxes and photocopiers should be checked regularly for prints which are not collected, especially in open office areas.

TRAINING

If necessary, application and hardware training should be available to all workstation personnel prior to the issuing of equipment or software, or as near as possible to the date it is received. Additionally, specific Information Security training is available if required.

LEGAL OBLIGATIONS

Adherence to this policy will enable you to comply with the main Information Security elements of current, relevant legislation. This includes, but is not limited to:

- Data Protection Act 1998
- The Computer Misuse Act 1990
- Copyright Designs and Patents Act 1984
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000

CONTACTS

For further information, please contact:

- Whinney Banks Primary School Tel: 01642 817713
  E-mail: whinneybanks@mcschools.org.uk

A SUMMARY OF THE

INFORMATION SECURITY POLICIES AND GUIDELINES

FOR

WHINNEY BANKS PRIMARY SCHOOL

FOREWARD

Whinney Banks Primary School is committed to full electronic service delivery wherever possible. In view of this, the confidentiality, security and accurate processing of data is, therefore of considerable importance to the Council.

The purpose of the policy statements and standards set out here is to act as guiding principles for the provision of the security, reliability and integrity of data and associated hardware within Whinney Banks Primary School.

Notwithstanding any partnership arrangements, all persons dealing with any aspect of Whinney Banks Primary School's information processing must be made aware of Whinney Banks Primary School's Information Security Policy and comply with its requirements. Non-adherence to the Information Security Policy may result in delays or curtailment of computer processing, which in turn may result in Whinney Banks Primary School suffering serious inconvenience and even financial loss.

Any officer failing to comply with the Information Security Policy will be subject to the appropriate disciplinary procedures.

Please note that this document is only a summary of the key policy elements. For more information regarding the policies and guidelines referred to below, please refer to the fuller version of the Policy, which is available at whinneybanks@mcschools.org.uk.

DATA PROTECTION

Whinney Banks Primary School is required to process personal information in accordance with the eight principles of the Data Protection Act 1998. For further information regarding Data Protection requirements, please refer to Appendix 1 of the full Policy document.

INFORMATION SECURITY

The objective of Information Security is to ensure service continuity and prevent loss and damage by minimising the impact of security incidents. Additionally, the purpose of this Policy is to protect the School's information assets from all threats, whether internal or external, deliberate or accidental. It is the responsibility of all staff to ensure that:
1) Information is protected against unauthorised access.
2) Confidentiality of information is assured.
3) Integrity of information is maintained.
4) Regulatory and legislative requirements are met.
5) Service Continuity plans are produced, maintained and tested.
6) Information security training is available to all staff, where necessary.
7) All breaches of information security, actual or suspected, are reported to and investigated by the Head Teacher.

E-MAIL USAGE

E-mail services are to be used for Whinney Banks Primary School related business. Whilst occasional personal e-mail is not prohibited, excessive personal use is not acceptable. Users should not send or solicit e-mails that are of a fraudulent, harassing, or obscene nature or contain inappropriate material.

Users should be aware that Whinney Banks Primary School's computer systems and communications may be monitored to ensure effective operation of the system and for other lawful purposes.

INTERNET USAGE

Access to the Internet is permitted to enable Whinney Banks Primary School employees to effectively and efficiently carry out their responsibilities and duties, and the Head Teacher must approve access. Occasional and reasonable personal use is permitted outside of core working hours. Downloading of software is not permitted unless authorised by the Head Teacher.

Please be aware that all access is fully logged and monitored to ensure effective operation of the system and for other lawful purposes. You should not visit or download any material from web sites containing illegal or unacceptable material, and any associated access may be subject to Whinney Banks Primary school's disciplinary procedures. Whinney Banks Primary School may utilise software that makes it possible to identify and block access to Internet sites, subject to agreed Policy.
Staff should not use Whinney Banks Primary School resources to print out web pages for information not related to work.

ANTI-VIRUS SECURITY

All Whinney Banks Primary School workstations and servers must be adequately protected against viruses. Where installed, anti-virus software must remain operational and you should not amend any associated settings without prior authorisation from IT Services. For equipment without anti-virus software installed, any electronic information being brought into Whinney Banks Primary School's IT environment (e.g. by floppy-disk, CD or memory stick) should be scanned for viruses on a suitably equipped system prior to use.
If you suspect that there may be a virus on your system, please inform the IT Help Desk immediately and await further instructions.

SYSTEM PASSWORDS

Your personal user identity must not be revealed to or shared with anyone else. If you must leave your computer unattended whilst logged on, you should secure your system by use of password protected screensavers or screen-locking facilities. Users will be held accountable for all activities carried out under their log on ID.
You must:
 Keep your password confidential.
 Use your own unique password/account/user-code to access Information Systems.
 Change passwords at initial login or when requested, or if your password may have been compromised.
 Avoid using passwords that may be easy to guess, for example by using sequential, obvious or recycled passwords.

You must **not**:
 Allow others to use your user ID or password(s).
 Write your user ID or password(s) down unless they are to be stored in a secure place.

HARDWARE

- Hardware (e.g. PC systems, laptops etc), issued to employees or agents of the Council, should be used only for the purpose intended and by the individual to whom it is issued. Such hardware should have no additions made to it without prior approval from IT Services.
- Staff with portable computer and communications equipment should protect them from the threat of theft or damage, and ensure that controls are in place to prevent sensitive information from being intercepted. Employees that travel with laptops should be cautious and endeavour to keep the items secure at all times.
- The physical connection of any equipment to the network will only be allowed after written approval by IT Services.
- Use of privately owned equipment is subject to a risk assessment and documented agreement for use prior to an employee being granted access to Whinney Banks Primary School's IT facilities.
- Any disposal of IT equipment should be performed by IT Services or other approved method.