Schools IT Services

IT Security Guidance

School:		
Date adopted by the Governing Body:		
Signed	**(Chair):**	
	(Headteacher):	

If you need this document in a different format please telephone 01942 827664 (internal 2664) or 01942 827186 (minicom)

Confident Place, Confident People.

April 2012

School IT Services – IT Security Guidance

1. What is this Guidance for?

1.1 To protect the School's information assets, equipment and systems, managed by the School's Information Technology Services (IT). This guidance also defines the security arrangements related to devices connected to the School's network.

This includes but is not confined to - PC's, laptops, printers, servers, telephones, PDAs, switches and routers.

1.2 To maintain the integrity and security of the School's network by ensuring that IT equipment is configured and used in a manner such that it:

- complies with all legal requirements;
- complies with all agreements with partners;
- continues to be accessible, available and usable, as normally required;
- maintains the integrity of data and keep it free from corruption; and
- does not bring the School into disrepute.

1.3 To provide clear information about the personal responsibilities of all owners and users of information managed by the School's IT Services.

1.4 To ensure that the benefits of widespread and effective use of IT facilities are achieved without compromising the confidentiality, security and integrity of the School's information.

2. The types of information this guidance covers

2.1 Information within this guidance means all data, programs, documents, spreadsheets, databases, electronic mail messages, images and maps of all types, regardless of how or where within IT systems the information is stored or managed.

2.2 All information is not of uniform value to the School and therefore different levels of protection against loss and disclosure are required. The following categories of information have been determined and used within this guidance:

- **Category 1**: temporary loss or unauthorised disclosure would have serious financial, operational, commercial or legal consequences for the School.
- **Category 2**: temporary loss or unauthorised disclosure would cause embarrassment or operational difficulty within the School and with its correspondents.
- **Category 3**: temporary loss would cause disruption within the School.
- **Category 4**: loss or unauthorised disclosure would cause little administrative embarrassment or difficulty within the School.

3. How School information must be looked after and your responsibilities

3.1 All users of IT facilities are individually responsible for protecting the School's information, equipment and systems from deliberate or reckless use and damage.

3.2 The School's Information Risk Policy * outlines the duties and responsibilities of all officers and applies to everyone who is authorised by the School to use any paper based or electronic system containing information provided for, owned, controlled, or administered by the School. In order to maintain public confidence and ensure the School complies with legislation you must maintain compliant standards of information security.

3.3 The Headteacher is the Information Asset Owner (IAO) for all information held within the school. For smaller schools, such as Primary or Special schools, the Headteacher will retain the responsibility as IAO. For larger schools, the Headteacher may nominate the senior IT manager as IAO. An IAO will also be named for each individual IT system within the school.

3.4 Headteachers must ensure that nominated Information Asset Owners (IAO) are made responsible for the ownership of all information within the IT systems for which they are responsible.

3.5 The IAO nominated for an IT system has responsibility for all the information stored in that IT system. This role includes the regular review of those individuals who have access to the data in those systems and the authorisation of data being transferred or shared.

3.6 Back-ups of data will be undertaken by the school's IT Services with Category 1 and 2 data being stored securely off-site from the location at which the operational information is maintained, wherever possible. It is the responsibility of the IAO to ensure that all data within their ownership is being adequately backed-up and can be restored.

3.7 Headteachers must ensure that all information for which they are responsible is classified generally in accordance with the categories in Section 2 and that appropriate procedures are in place to maintain the confidentiality of the information and to recover from the temporary or permanent loss of the information or supporting equipment.

3.8 Access to systems and information will be administered by the nominated representative of the Headteacher on behalf of and as authorised by the Information Asset Owner for those systems.

3.9 The Headteacher, or their nominated representative, will monitor all activity by the School's IT Service staff within live systems.

4. How School information must be kept secure

4.1 Information must be stored, transferred and processed in accordance with:

- The School's Data Protection Policy *
- The School's Information Risk Policy *
- The School's Use of Mobile Data Devices & Equipment Policy *.

4.2 All information held within the School systems is the property of the School and the use of IT systems is monitored and logged. This may be carried out through a Securus system or similar. Securus is a monitoring system used by many Wigan Schools.

4.3 The Headteacher may authorise appropriate people to access any information including data, logs, images, messages and recording. Information held on School systems may be subject to disclosure to the general public under the Freedom of Information procedures.

4.4 All School data must be stored on secure back-up systems on-site, unless an alternative location is authorised by the Headteacher or their representative, which must be compliant with the School's Data Protection Policy *. A record must be kept of all backups made and tests made periodically to ensure it can be restored. All data stored off site must be encrypted to maintain security of the information held.

4.5 No information may be stored on portable memory devices, except where permitted by the School's Use of Mobile Data Devices & Equipment Policy *

5. How access to School's information must be managed

5.1 Access to and the use of School information must be controlled in accordance with the School's Data Protection Policy * and Schools IT Acceptable Usage Guidance *.

5.2 Any users of the School's network will select strong passwords – with advice from the School's IT Services.

5.3 Each user must have their own User-ID and password and must only use these in accordance with the terms of the IT Acceptable Usage Guidance *. A user may not disclose any personal password to another person neither should they make any record of them.

5.4 In accordance with Section 7 of the Financial Regulations and Standing Orders for Schools, auditors nominated by the Board of Governors will have access as necessary to any information and applications systems.

5.5 Only persons with a genuine business requirement and permanent need may be given permanent access to networks and application systems. Those persons with a temporary need will be granted temporary access. The Headteacher as Information Asset Owner (IAO) or nominated representative can grant access. The Headteacher will be the final arbiter of need.

5.6 Access by employees of outside bodies, to the School's network or IT facilities, must not be given without prior agreement from the Headteacher. The employing organisation of any person given access to the School's network, IT facilities or

information must comply with this Guidance and ensure that their staff adhere to its requirements.

5.7 The Headteacher or nominated representative must be notified in writing of all leavers who have access to the school network system, in order that access to the individual is withdrawn. Likewise if staff transfer from one school or area of the school to another, the Headteacher must be notified of this by the department they are leaving, so that access to IT systems can be reviewed.

5.8 Only people authorised by the Headteacher may use hardware or software to monitor, investigate or inspect systems, networks or data, except for the provision of 5.5 above.

6. How School software must be managed

6.1 All computer programs and information developed for, or purchased by, the School are for the sole use of the School and its business. Personal use of these systems must only take place in accordance with the terms of the School IT Acceptable Usage Guidance *. Any use outside of this must be by express permission of the Headteacher.

6.2 Only software approved by the Headteacher, or nominated representative may be installed on equipment and devices connected to the School's network. Where a licence is issued for a number of users, this must be monitored to ensure that the licence conditions are not breached.

6.3 All modifications to operational programs must be approved by the Headteacher, or nominated representative, who must be satisfied that testing has been completed satisfactorily.

6.4 All software should be maintained and updated to ensure it is free from security weaknesses. Software which cannot be maintained or updated must be removed from use if significant security weaknesses are identified.

6.5 Software must only be installed, used, duplicated or transferred in accordance with the appropriate license agreement.

7. How School equipment must be managed

7.1 Headteachers are responsible for IT facilities used by their people and for ensuring its proper use. The only use of IT facilities for purposes not directly concerned with the School's business, is for personal use as described in the School IT Acceptable Usage Guidance * and any exceptions to this must be agreed by the Headteacher.

7.2 All items of equipment must be security marked and logged within the asset register in accordance with the School's risk management policies.

7.3 The purchase of IT equipment must be through the Headteacher or nominated representative and only equipment authorised by the Headteacher may be connected to the School's network. This equipment must be installed and configured in an approved manner.

7.4 All equipment and devices connected to the School network must be maintained and operated in a manner approved by the Headteacher and only persons approved by the Headteacher may undertake maintenance or modification of IT equipment.

7.5 Only persons approved by the Headteacher or nominated representative may be granted the role of 'Administrator' of a workstation or other device connected to the Schools network.

7.6 Equipment must not be left unattended in vehicles or outside of school premises. In addition, equipment should not be used in public areas that may display information which is subject to the Data Protection Act, to unauthorised persons.

7.7 IT equipment and devices, which are considered to be redundant or obsolete must be inspected by the Headteacher's nominated representative, who, in conjunction with the governing body, will make the final decision as to whether they are redundant or obsolete.

7.8 All obsolete or redundant School IT equipment and devices must be dealt with in accordance with the Confidential Waste Policy for Schools ** – section seven – 'How do I dispose of electronic IT waste?'.

8. What happens if this and the associated policies are breached?

8.1 All users of the School's IT facilities must report suspected or known breaches of this Guidance to the Headteacher or nominated representative

8.2 The Headteacher, or nominated representative, will be responsible for investigating reported or suspected breaches. They may request advice and assistance from HR Casework and Advisory Team, within HR & OD Services, or from Audit Officers within Resources Directorate, where appropriate.

8.3 Users carrying out activities in breach of this School IT Security Guidance, and associated policies, will also be regarded as being in breach of the School's Staff Code of Conduct. This would result in action under the School's disciplinary procedure and may constitute gross misconduct where appropriate. This could ultimately lead to dismissal from employment and users may also be subject to civil and criminal proceedings.

9. How can I find out more about any aspect of this Guidance?

9.1 Further information and guidance can be obtained by contacting the IT helpdesk.

This Guidance needs to be read in conjunction with:

- School Data Protection Policy *
- Schools IT Acceptable Usage Guidance *
- Use of Mobile Data Devices & Equipment Policy *
- Schools Information Risk Policy *
- Confidential Waste Policy for Schools **

* It is recommended that all schools develop each of these policies, if they haven't already done so.

** The recommended Confidential Waste Policy for Schools is available on the intranet, under Children and Young People's Services, School Information, Pro-formas.