The Westminster School

Information Security Policy 2015/2016

Approved by Governing Body on:	12/02/15
Signed by Chair of Governors:	
Head Teacher:	C A Hill B.E.d..N.P.Q.H.
Lead Personnel:	B Taylor
Date of Review:	

1. Introduction

Information is an important asset and of significant value to The Westminster School. The School must protect its information from threats – internal and external, deliberate or accidental that could disrupt the work of the School or infringe the rights of employees.

Information Security involves the protection of information for:

Confidentiality	Keeping information out of the wrong hands
Integrity	Making sure information is accurate and complete
Availability	Ensuring reliable and timely availability of information and services

This Policy has been developed using the internally recognised standard for information security known as ISO27001. This takes a risk based approach to upholding the 3 key principles as outlined above.

Whilst the aim is to provide facilities for employees to use freely in pursuit of their job, there are however, management and legal issues which must be borne in mind to ensure the effective and appropriate use of information.

Information security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

All information created or processed on behalf of the school is regarded as being owned and accessible by the school as part of its 'business record'. This Policy focuses on electronic information processed by computer and on protecting the technology used to store, process and transmit it. However the principles apply equally to other forms of information including paper records, microfiche and spoken conversation (including voice mail).

The Westminster School does allow appropriate non-work related use of computer resources including email and internet. However, employees should be aware that any material that they create, store, send or receive may be monitored in accordance with the School's policy regarding this subject.

The Policy should be read and used in conjunction with all relevant supporting information published by Becta (Copyright – Becta, March 2009) – information specified later.

2. Statement of Support

The objective of Information Security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.

The purpose of this Policy is to protect The Westminster School information assets from all threats whether internal or external, deliberate or accidental.

The Governing Body, Head Teacher and Management Team have approved the Information Security Policy.

It is the policy of the organisation to ensure that:

- Information is available for legitimate use while being protected against unauthorised access;
- Confidentiality of information is assured;
- Integrity of information is maintained;
- Regulatory and legislative requirements are met;
- Business Continuity plans are produced, maintained and tested;
- Information security training is available to all staff;
- All breaches of information security, actual or suspected, are reported and investigated;
- Specifically for this Policy - the seventh principle of the Data Protection Act is upheld at all times.

Business requirements for the availability of information and information systems will be met.

It is the responsibility of each member of staff to adhere to the policy.

Signed:…… Date:……

Print Name:……

Position:…….

3. What do we mean by information?

Information is a generic term used throughout this Policy. It can take many forms e.g. electronic, written or vocal. It would be wrong to assume that information in any form warrants the highest level of protection or may never be disclosed as described in this Policy.

Therefore in applying this Policy everyone handling information must take a pragmatic and sensible approach, e.g. a publicly available newspaper or leaflet does not warrant anything near the same protection as something like Child Protection and therefore the rules of not keeping it on an unattended desk would be absurd.

Therefore common sense and professional judgement must be applied taking into account other demands such as the Freedom of Information Act. For the avoidance of doubt, other supporting resources and contacts are available as described throughout this Policy.

4. General Principles

The Westminster School has a significant investment in ICT and information. The school is increasingly dependent upon the information it holds and processes. The loss of information or its ICT processing facilities could lead to significant additional costs, resource burden and damage to the Schools reputation as a result of:

- Business activities being fully or partially suspended (if the information is personal data, formal intervention from the Information Commissioner);
- Having to recover information or ICT facilities and equipment;
- Unauthorised disclosure of protected information relating to individuals being made available to 'interested parties';
- Fraudulent manipulation of cash or goods.

Always remember:

- Information Security is your personal responsibility. Know the rules for handling the information in your care. Stick to those rules without exception;
- Before making information available to anyone else, make certain you have the authority, including the legal power, to release it;
- Never access information unless it is part of your job and you have a business need to do so;
- Never give out information via the telephone or in any other way unless you are absolutely sure who you are giving it to, that it is adequately protected whilst in 'transit' and that the recipient is entitled to receive it.

When in school:

- Never leave information out on your desk when you are not present;
- Always 'lock' your computer before leaving your desk unattended;
- Lock and remove the keys from cabinets or other storage units if you leave the office unattended and access to information may be compromised;
- Choose your passwords carefully and never let anyone else know them;
- Challenge anyone you see in the building who should not be there – do not allow anyone to 'tail gate' you through security doors.

On the move:

- Never take information out of the office unless you need to. Keep your ICT equipment – laptops, portable media (e.g. memory drives, CDs), telephone, smart phone and all paperwork secure at all times;
- Never leave equipment or documents in a vehicle when it is unattended and always travel with it locked securely and out of sight;
- When working in a public place, make sure you are not overheard and that information cannot be seen by others.

Transmitting information:

- Always make sure you know what Protective Marking the information you are using should have and always comply with that level of protection;
- Be certain you are sending only what you absolutely need to send and no more;
- Ensure the method of transfer is appropriate to the protection of that information and if in any doubt do not use it;
- Data Processing Agreements must be in place for any information processed by a third party and the School remains as the recognised Data Processor.

5. Scope

This Policy defines security standards which apply to all employees, contractors, third parties and temporary staff working on behalf of The Westminster School.

This Policy is relevant to all information systems whether they be computer or paper based. It covers all devices capable of holding information. This includes, but is not limited to information:

- Stored on computers
- Transmitted across networks
- Printed out
- Written on paper
- Sent by fax
- Stored on tape, disc or other electronic means
- Spoken in conversation e.g. by telephone
- Sent via email
- Memory sticks or other portable storage devices (encrypted or otherwise)

6. Rationale for this Policy

Our Information Security Policy is in place to ensure that:

- Information owned or processed by the School is protected against threats, be they internal or external, deliberate or accidental;
- Confidentiality of information is assured – we will protect our information from unauthorised access, use, disclosure or interception;
- Integrity of information is maintained – we will protect information from unauthorised changes or misuse, so that it can be relied upon as accurate and complete;
- Availability – information is available when and where it is needed;
- Legal and regulatory requirements are understood and met;
- Information and training on information security is up to date and available to all employees.

7. Relevant Legislation and Guidance

A detailed framework of relevant legislation:

Legislation	**Areas Covered**
The Freedom of Information Act 2000	Public access to School information
The Human Rights Act 1998	Right to privacy and confidentiality
The Electronic Communications Act 2000	Cryptography, electronic signatures
The Regulation of Investigatory Powers Act 2000	Directed surveillance and access to communications data
The Data Protection Act 1998	Protection and use of personal information
The Copyright Designs and Patents Act 1988	Software piracy, music downloads, theft of School data
The Computer Misuse Act 1990	Hacking and unauthorised access
National Immigration and Asylum Act 2002	Home Office Powers to receive information held by employers about employees and ex-employees
Social Security Administration Act 1992	Police rights to information held by employers about employees and ex-employees

8. Managers and Individuals Responsibilities

All School Managers are directly responsible for promoting, publicising and implementing the Policy within their school and for ensuring adherence by their staff or appointed contractors.

It is everyone's responsibility to make themselves aware of this Policy and to adhere to it.

Information security breaches (suspected or definite) should be reported to the Head Teacher as soon as possible. In addition, detailed records of all information security breaches will be maintained. A formal notification of any breaches must be sent to the Council's Data Protection Officer.

Deliberate breaches of this Policy are regarded as a disciplinary matter. The School reserves the right to take legal action in relation to a serious breach of Policy.

If you do not understand the implications of this Policy or how it applies to you, refer to the good practice guides produced by Becta on behalf of the DCSF.

9. Method of Monitoring

Periodic checks of user accounts and e-mail accounts.

10. Review and Revision

This Policy will be reviewed annually.

When changes are made to any aspect of the Policy, employees will be informed.

11. Supporting Good Practice Guides

This Policy outlines the top level rules for information security. Good Practice Guides produced by Becta (Copyright Becta, March 2009) on behalf of the DCSF. These can be accessed from the following Becta Website.

http://www.becta.org.uk/schools/datasecurity

These include:

- Good practice in information handling: Data security dos and don'ts
- Good practice in information handling: Keeping data secure, safe and legal
- Good practice in information handling: Data encryption
- Good practice in information handling: Audit logging and incident handling
- Good practice in information handling: Secure remote access