Kirton Lindsey Primary School

Information Security and Confidentiality Policy

January 2018

CONTENTS

1. Introduction

Information stored and processed by the school is a valuable asset. Without adequate levels of protection, confidentiality, integrity and availability the school will not be able to fulfil its obligations including the provision of education and meeting legal and statutory requirements.

The school's information exists in many forms including:

- Hardcopy documents on paper and sent by fax
- Electronic information stored on computers, remote servers, mobile devices, tapes, microfilm, CDs, external disks and USB portable storage devices
- Verbal information (face to face conversations and over the telephone)

The school is committed to preserving the confidentiality, integrity and availability of information assets:

- For sound decision making
- To deliver quality education services to children and young people
- To comply with the law
- To protect the school's reputation as being professional and trustworthy
- To safeguard against fraudulent activity
- To keep children, staff and the school safe

This policy sets out the school's commitment to information security and confidentiality and provides the guidelines and frameworks for ensuring all forms of information, supporting systems and networks are protected from security threats such as malicious software, unauthorised access, computer misuse, information technology failures, human error and physical security threats.

2. Purpose

The purpose of this policy is to protect the school's information from all threats whether internal or external, deliberate or accidental. The policy sets out the controls and requirements that will protect a wide range of information that is generated, shared, maintained and ultimately destroyed or archived.

The purpose of Information security and confidentiality is to preserve an appropriate level of:

- **Confidentiality:** to prevent unauthorised disclosure of information
- **Integrity:** to prevent the unauthorised amendment or deletion of information
- **Availability:** to prevent the non-availability of information and the unauthorised withholding of it.

3. Scope

This policy applies to all information assets held by the school irrespective of their form and covers all locations into which the school's information is taken and/or accessed.

The scope of this policy extends to all schools where it has been adopted by the governing board and to:

- Staff
- Contractors, agencies and partner organisations operating on behalf of the school or on the school's premises.

4. Legal Framework

The school must comply with all relevant statutory UK and European Union legislation, including:

- Human Rights Act 1998
- Data Protection Act 1998
- Common law duty of confidence
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Regulations 2000
- Waste Electrical and Electronic Equipment (WEEE) Directive

The requirement to comply with this legislation extends to all employees who are held personally accountable for any breaches of information security for which the School is responsible.

5. Technical Compliance

The Data Protection Officer will ensure that information systems are checked regularly to ensure they are still protected by the most up to date security available.

6. Linkages with other policies and procedures

This policy is supported by other policies including the following:

- Request for Information Policy
- Records Management Policy
- School’s Complaints Policy.

7. Reporting structure

The following are key information security and confidentiality roles:

1. The Data Protection Officer is the senior responsible member of staff for information security/risk and leads the school's response by:

    - Fostering a culture for protecting and appropriately using information
    - Providing a focal point for managing information risks and incidents
    - Ensuring that all information assets and the records they contain are managed
    - Ensuring that employees have the appropriate level of access to the information they need and are familiar and compliant with their responsibilities under the Data Protection Act 1998.
    - Ensuring that risk assessments are carried out and appropriate controls implemented.
    - Ensuring that actual or potential security incidents are recognised and appropriate action taken to stop the incident, investigate and make changes where necessary.
    - Ensuring that contractors, partner organisations and third parties have appropriate and satisfactory systems and procedures in place and agreed terms and conditions consistent with this policy before doing business with the school.
    - Ensuring staff are regularly trained to an appropriate level and comply with this policy.

2. The Administrator deputises for the Data protection Officer.

8. General Data Protection Regulation 2018

All organisations including schools that process (handle) personal information must comply with the eight principles of the Data Protection Act. Personal information is that which could identify someone either directly or by being combined with other easily accessible information. A summary of the principles is following:

Personal information should be:

1. Fairly and lawfully processed;
2. Obtained for specified purposes and not used for other incompatible purposes;
3. Adequate, relevant and not excessive;
4. Accurate and up to date;
5. Not kept for longer than necessary;
6. Processed in line with the rights of individuals;

7. Kept secure;
8. Not transferred to countries outside of the European Economic Area unless adequate protection is assured.

9. Notification, Privacy Notices and Risk Assessments/Privacy Impact Assessments

The Information Commissioner's Office (ICO) is the regulator for the majority of information related legislation. Schools must notify the ICO of the purposes for which they are processing (handling) personal information. This is an annual requirement of the Data Protection Act 1998 and a set fee must be paid.

Schools must publish a Privacy Notice that explains why the school is collecting personal information, who will look after it and what will happen to it. Privacy notices will also be considered for publications, forms and leaflets issued by the school where the collection of personal information is involved.

Schools will ensure that information is accurate at the time of capture and that it is subsequently maintained to ensure accuracy, integrity and consistency. An annual risk assessment will be carried out by the school on all major information assets, such as IT systems, record storage facilities and processes to assess and record the risk to personal information. These will be documented along with any action required to reduce the risk to personal information. The same risk assessment will be carried out before the introduction of new systems and ways of working. These risk assessments are sometimes called Privacy Impact Assessments.

10. Security Incidents

School employees will inform the Data Protection Officer or an appointed deputy if they suspect there has been or might be a security incident that could result in the school's personal information being lost or seen by someone who should not see it.

The following are factors that may lead to a security incident:

- Negligence or human error;
- Unauthorised or inappropriate access, such as accessing information you are not permitted to see or using someone else's password;
- Loss or theft of information or equipment;
- Systems or equipment failure;
- Environmental factors, such as fire or flooding;
- Accessing information without a business reason to do so;
- Insufficient physical security;
- Insufficient access controls;
- Lack of training;
- Hacking;

- ‘Blagging’ or ‘social engineering’ in order to gain access to information.

The school will immediately investigate:

- Speedily and efficiently;
- Consistently;
- Keeping damage to a minimum;
- To reduce the likelihood of a recurrence.

11. Key Policies and Procedures

Procedure	Summary
Home working / remote working	• All data related to individuals must be stored on the school server and not on any hardware. . • All necessary precautions must be taken to ensure the security of hard copy information that is taken off school premises. • All home working and remote working should be carried out in compliance with this policy and have the authorisation of the headteacher or deputy.
Procurement of services	• Ensure that Data Protection and Freedom of Information requirements are clearly specified within the conditions of contract and service specification for all relevant procured services. • Ensure that the pre-qualification/evaluation of prospective suppliers includes where appropriate consideration of capability for ensuring Data Protection. • Ensure that due regard is given to Data Protection as part of contract monitoring and management. • Consider the implications of sub-contracting and ensure that the above requirements are passed through the relevant supply chain. • Ensure that third parties have adequate controls in place with regards to off site/remote storage of school information.
Disposals	• To comply with the Waste Electrical and Electronic Equipment (WEEE) Directive and ensure that sensitive data is not accidentally released. • When disposing of any sensitive and confidential information use an approved confidential waste contractor or another secure method of disposal, such as cross-cut shredding. • If working at home be aware of the need to comply with the above disposal methods. If no secure disposal methods are available, sensitive information should be transported to the school for secure disposal.

Procedure	Summary
	• It is important to keep the waste in a secure place until it can be collected for secure disposal or cross-cut shredded. Never put sensitive and confidential waste in any normal waste bins.
Systems and Software	• All school information processing systems must be formally authorised by the headteacher. User access to systems must be adequately controlled using unique complex passwords and appropriate access rights. User access rights must be regularly reviewed to ensure they are still appropriate. • Users are responsible for keeping their passwords confidential at all times, and must not disclose passwords to anyone, including their managers. Written down passwords shall be discouraged, unless documentation is completely inaccessible to other persons. Weak passwords must not be used. • Users must not attempt to access systems or records within systems which they have not been formally authorised to access. • Users must not bypass, disable or subvert system security controls. • Unauthorised equipment must not be connected to the school's network. • Computer systems and software must only be used for purposes for which they are designated. • USB ports should be restricted and only permit the use of approved and encrypted devices or accessories such as mice and chargers. • Software must only be used in compliance with the terms of any contractual or licence agreements. • The school will have sole ownership and copyright of all programs and data it has developed, unless prior written consent has been given otherwise. • Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is strictly forbidden. • All staff with IT access must undergo the school's Information Security training package and this must be part of the induction process for new staff. • Managers must ensure that when any staff leaves, all school equipment and access codes or keys are returned. Access to IT systems must be removed. • All users must inform the Data Protection Officer or deputy if they detect, suspect or witness an incident which may be a breach of security.

Procedure	Summary
	• All users must be aware that the network is monitored.
Information Handling	<u>Storage</u> • Information must not be put at risk of damage or theft, and must be stored securely and access allowed only to those who need, it for legitimate purposes and in accordance with the Data Protection Act 1998. For example: o Records should be stored in secure buildings with access controls to the building, specific floors and individual offices. o The location of any stored records should be sited to avoid unauthorised access, damage, theft and interference. o Stored records must not be removed or moved to another location without authorisation from the Data Protection Officer or deputy. o Electronic information must to be stored on the school network unless alternative storage (e.g. Cloud) is authorised. <u>Communication</u> • Extra care should be taken when printing sensitive information or sending/receiving faxes. When sending sensitive information a test fax should be sent prior to sending the information. Print release security controls will be used whenever possible but in any areas without multi-functional devices ensure printed sensitive information is not left unattended. • Voicemail may contain personal and sensitive information and therefore passwords should be kept secure. • File Sharing products or 'apps' that are not approved by IT Services must not be used for council business. <u>Portable hardware including laptops, mobile devices & tablets</u> • Equipment taken off site must be locked away and kept out of sight when left unattended. • Users shall ensure that unauthorised persons are not able to view school's information on portable devices and shall protect access by locking computers when unattended. <u>Records Management</u> • Records are a key resource for the effective operation and accountability of the council. It is also recognised that some records will over time become of historical value and need to be identified and preserved accordingly.

Procedure	Summary
	• Hardcopy records that do not need day to day access should be stored away from the immediate workplace. • Any hard copy or electronic records temporarily stored away from the usual storage location must be returned there as soon as is practicable. <u>Removable media</u> • To prevent data loss the use of any removal media must be approved by the Data Protection Officer or deputy with a strong business case for use. • Staff must only use mobile media to store or transfer personal and sensitive council information if there is no other more secure means available e.g. Government secure GCSx email. • Only media with a sufficient level of encryption may be used to temporarily hold personal and sensitive school information. <u>Office/desk security</u> • Staff should maintain a clear desk policy and ensure that all personal and sensitive information is kept secure: o To minimise the risk of mixing up information and accidentally releasing it to someone who should not see it only information relating to the current task should be on the working area of the desk at any one time. o Personal and sensitive information including phone numbers, passwords, financial records, notes on meeting times, places and subjects must not be left unattended o Mobile phones can contain sensitive personal information and have their call histories compromised and therefore should be kept secure using a pin number and/or passcode at all times and not left unattended o Keys and access cards should not be left unattended as they can give intruders access to restricted areas o Positioning of desks, furniture and visual display boards should be carefully considered to prevent sensitive information being visible to unauthorised people. o Personal and sensitive information should not be left on white boards or notice boards. o When leaving desks for short periods all users must use 'Ctrl, Alt and Delete' to lock computers. When leaving desks for long periods users must ensure they are logged off the network.

Procedure	Summary
Information Security Classification	Identification of Sensitive Records • Records that contain sensitive or personal information should be marked so that it is immediately apparent that they need to be protected.

12. Information Sharing and Information Access/Disclosure

Personal and confidential information will be shared within the school and with other organisations in line with the law and where there is a need or obligation to do so. Where there is a need to share information with external organisations the information sharing will be governed either under the terms of a contract and/or an information sharing or information access / disclosure agreement. Schools will consider signing up to The Humber Information Sharing Charter and using the template within it to set up information sharing agreements.

13. Audit

The Information Security Policy, standards and procedures will be audited periodically as part of the annual internal audit work plan.

14. Monitoring and Review

The current version of this policy and any supporting information can be found on the data security page on the school website – http://www.kirtonlindseyschool.co.uk/data-security/ along with any supporting information. This policy and all supporting procedures will be reviewed as it is deemed appropriate but no less frequently than every 12 months, with re-approval every 3 years.

Adopted by the Governing Body at their meeting on: