Hardenhuish School

Information Security Policy

If you would like any policy in a more accessible version, please contact the Office Manager

Approved: May 2018
Review Date: May 2019
Committee: P and R

Information Security Policy

1. Introduction

Staff at Hardenhuish School have increasing access to a wide range of sensitive information. There are essentially two types:

- personally sensitive data concerning the staff, pupils and other stakeholders, and
- commercially sensitive & operational information.

It is important to ensure that both types of information are managed in a secure way at all times.

Three questions can be used to quickly assess the need to treat any information securely:-

a) Would disclosure/loss place anyone at risk?
b) Would disclosure/loss cause embarrassment to an individual or the school?
c) Would disclosure/loss have legal or financial implications?

If the answer to any of the above is "yes", the information contains personal or commercially sensitive information and needs an appropriate level of protection.

2. Definition of Information Security

Information security means safeguarding the School's information from unauthorised access or modification to ensure its:

- **Confidentiality** – ensuring that the information is accessible only to those authorised to have access
- **Integrity** – safeguarding the accuracy and completeness of information by protecting against unauthorised modification
- **Availability** – ensuring that authorised users have access to information and associated assets when required

3. Statement of Intent

Information is an important asset. The Governing Body and the management of Hardenhuish School are committed to preserving the confidentiality, integrity, and availability of our school's information assets:

- For sound decision making;
- To deliver quality education;
- To comply with the law;
- To meet the expectations of our stakeholders;
- To protect our reputation as a professional and trustworthy organisation.

4. Scope

This policy applies throughout the lifecycle of the information from creation, to storage, use and finally to disposal. It applies to all information including:

- Information stored electronically on databases and applications, e,g, email or computers
- Information stored on removable media such as hard disks, CD rom, memory sticks and other similar media

- Information transmitted on networks
- Information sent by fax or other communication methods
- All paper records
- Microfiche, visual and photographic materials including slides and CCTV

5. Legal and regulatory requirements

Employees, third parties and partners who have access to the school's information assets will abide by legislation relevant to information security including:

- Common Law Duty of confidentiality
- Data Protection Act 2018
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Copyright, Designs and Patents Act 1988
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Civil Contingencies Act 2004

6. Roles and Responsibilities

The Governing Body is ultimately responsible for ensuring that information security is properly managed.

The Headteacher is responsible for:

- The development and upkeep of this policy;
- Ensuring that this policy is supported by appropriate documentation and procedural instructions;
- Ensuring that documentation is relevant and kept up-to-date;
- Ensuring that this policy and subsequent updates are communicated to relevant departments and personnel;
- Ensuring that information security arrangements are regularly reviewed to ensure that they comply with this policy and other security policies and standards in place.

Information security is everyone's responsibility and all employees, third parties and partners who have access to the School's information are required to comply with this policy.

7. Information and Records

The amount of information held by the school will be kept to a minimum. Personal data held by the school will be routinely assessed to consider whether it still needs to be retained in accordance with the School's Retention Schedule.

Personal data held by the school will be securely stored electronically or in hard copy in secure filing cabinets. Where it is necessary to transfer data, in accordance with the data protection principles, it will be sent by secure means, e.g. it will be encrypted.

8. Security Measures for any sensitive information held by the School.

Staff are responsible for ensuring that they password protect or encrypt any data that is determined to be personal or commercially sensitive in nature. This includes data held on desktop computers, laptops and memory sticks.

Staff must not remove or copy sensitive school data unless the media is encrypted, transported securely and stored in a secure location.

Sensitive and personal data must not be transmitted in unsecured emails. Where it is necessary to transfer such data, this transfer must be made via secure web portals. If this is not available, the information must be at the least password protected and preferably encrypted before sending via email. If this method of transmission is used, the password must be sent by other means and on no account included in the same email.

The ICT Support Manager is responsible for:

- Ensuring that data (pupil records, SEN data, contact details, assessment information) is backed up, encrypted and stored in a secure place – e.g. fire safe/remote backup.
- Securely wiping hard drives of PCs and laptops before transferring ownership or disposal.
- Ensuring that the School's wireless network is secure at all times.

The school will keep a record of what data and information is held, who has access to it, how it is retained and disposed of.

Staff are responsible for:

- Adhering to the school's Email and Computer Acceptable Usage Policy
- The security of sensitive information

Remote access to data for staff is facilitated by the remote desktop. Personal and confidential information must not be stored on a personal (home) computer.

The school will keep necessary pupil and staff information in accordance with its Retention Schedule. The school securely deletes commercially sensitive or personal data in accordance with that schedule.

All staff are trained to understand the need to handle data securely and the responsibilities incumbent on them.

9. Action in the event of a policy breach

All employees, third parties, and partners with access to the School's information assets have a responsibility to promptly report any suspected or observed security breach.

Security incidents that result from a deliberate disregard of any security policy requirements may result in disciplinary action.

10. Monitoring

Information security will be monitored on a continuous basis with action taken to reinforce security if required. Any breaches will be reported to the Governing Body.