Nursery School & Children's Centre

Data Protection Policy

2015/2016

For staff and contractors tasked with implementing data security

Policy Owner/Approval	Alison Hindle
Policy Version	1.1
Version Status	Work in Progress
Next Review Due	Autumn 2016
Policy Location	C:\Users\ahindle\Documents\Policies\HNS&CC Policies & documents

Contents

1 Introduction

This policy provides core security principles that Highfield Nursery School & Children's Centre follows to ensure that Setting, LCC and Government assets (information, property and staff) are secured in a proportionate manner and that information (including personal data) can be shared confidently, knowing it is reliable, accessible and secured to agreed standards.

The underlying principle of our policy is that through a combination of technical and procedural solutions, Highfield NS&CC (the Setting) will do everything within their power to ensure the safety and security of any personal data (or data that is important to the secure running of the setting).

In following this policy, the reader we aim to identify:

- data and information assets (data, stored in any manner, which is recognised as important or 'valuable' – not just in financial terms – or important to the setting), with named owners responsible for them
- a framework for ensuring data is correctly marked, managed and secured
- methods for the systematic assessment of risks and recording of data loss so that appropriate mitigating measures can be established.

2 Who is responsible and what data handling changes are required?

Data Handling Procedures in Government highlighted two roles that have responsibility for information security risk management. Highfield NS&CC already have staff with different titles who carry out these roles. However, we have adopted the titles below (and the responsibilities attached to them).

2.1 Senior Information Risk Owner (SIRO)

SIRO: Alison Hindle

The Senior Information Risk Owner (SIRO) is a senior member of staff who is familiar with information risks and the organisation's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- They own the information risk policy and risk assessment
- They appoint the Information Asset Owners (IAOs)
- They act as an advocate for information risk management.

The Office of Public Sector Information has produced *Managing Information Risk* [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support SIROs in their role.

2.2 Information Asset Owner (IAO)

IAO: 1 Business Finance Officer

IAO: 2 Administration Officer

IAO: 3 Health Development Coordinator

The Setting has identified information assets. These include the personal data of children and staff; such as assessment records, medical information and special educational needs data. Information assets also include non-personal data that could be considered sensitive if lost or corrupted, such as financial data, commercial data, research data, organisational and operational data, and correspondence. The 'value' of an asset is determined by considering the consequences likely to occur if it is lost or compromised in anyway, such as identity theft, adverse publicity or breaches of statutory/legal obligations.

An information asset is regarded as the collection of data or an entire data set. It is important to distinguish between an information asset and the information (usually a subset of the asset) that needs protecting. For example, reports run from a core information asset, such as a management information system, are not information assets themselves.

The Setting has identified an Information Asset Owner (IAO) for each asset or group of assets as appropriate. For example, Highfield's management information system is identified as an asset and has an IAO.

The role of our IAOs is to understand:

- what information is held, and for what purposes
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. Typically, there may be several IAOs within an institution, whose roles may currently be those of e-safety co-ordinator, ICT manager or information management systems manager.

Although we have explicitly identified these roles, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

2.3 Recommended changes

To adequately protect data, the Setting may need to make operational and technological changes. Some can be accomplished quickly with existing resources; others will require extra investment and the help of ICT and managed service suppliers primarily using the LCC provider Westfield Centre. In any given organisation, Information Asset Owners will need to work out the level of change required by carrying out a thorough information risk assessment. Highfield will also need to make staff more aware of data security with training. They may also need to put in place systems and procedures for:

- protectively marking data
- encryption
- audit logging
- responding to security incidents
- secure remote access (using two-factor authentication where needed)
- reviewing contracts for data protection and processing (including cross-border data flows if data is processed abroad)
- reviewing user access requirements for remote access to, and storage of, secured data.

As new technologies are developed, the Setting will need to develop new systems and procedures to maintain and improve data security.

3 Information risk assessment

It is important that the Setting conducts thorough risk assessments on the assets they hold. This will help plan security measures that are practical and proportionate to their specific size and risk profile.

3.1 Conducting an information risk assessment

When working out criteria for assessing risk the Setting will need to take into account:

- the assets involved
- legal requirements (such as the Data Protection Act 1998)
- the practicalities of running the Setting day to day
- the impact of incidents on reputation in the community.

Organisations should then identify, describe and prioritise risks against these criteria. The first step in identifying risks is for Information Asset Owners to list information assets that contain personal data or data valuable to the organisation.

Steps in identifying risks include identifying:

- assets

- threats
- existing controls
- vulnerabilities
- consequences.

Once organisations have identified risks they can estimate the size of those risks, that is, the combination of consequence and likelihood.

4 Good practice in information handling

Using technical good practice should help the Setting secure data and so reduce the risk of security incidents. They will also help meet the minimum requirements of *Data Handling Procedures in Government*.

4.1 Impact levels and protective marking

The Government has published *HMG Security Policy Framework* [http://www.cabinetoffice.gov.uk/spf], which recommends that the Government Protective Marking Scheme is used to indicate the sensitivity of data. The scheme is made up of five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. Most learner or staff personal data that is used within educational institutions will come under the PROTECT classification but an increasing amount of data is classified as RESTRICTED and CONFIDENTIAL.

At the Setting we are continuing to look at the practical issues involved in applying protective markings to electronic and paper records and are working to find ways of automatically marking reports and printouts.

4.2 Data encryption

It is a legal requirement of the Data Protection Act 1998 to protect and secure personal data. The Information Commissioner's Office (ICO) recommends that portable and mobile devices (including media) used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

The Setting encrypts any personal or sensitive data that is removed or accessed from outside an approved secure space. Examples of approved secure spaces include physically secure areas in HNS&CC, the local authority and the premises of support contractors. This applies to both communication links (for example, SSL or IPSec VPNs) and to files held on electronic storage media (for example, hard drives, CDs, DVDs, USB sticks and memory cards). In particular:

- when sensitive or personal data is required by an authorised user from outside the Setting's premises (for example, by a member of staff to work

from their home), they should preferably have secure remote access to the management information system or learning platform
- if secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- the Setting or users must securely delete personal or sensitive data when it is no longer required.

In order to comply with the intent of *Data Handling Procedures in Government*, HNS&CC takes a comprehensive approach to data security. Other important measures include identification, authentication, authorisation, accountability and audit.

4.2.1 Encrypting devices and media

The Setting can encrypt personal data on a device – for example, a laptop – using either full disk encryption (also known as whole disk encryption) or file/folder encryption (also known as file system level encryption). In general, the Setting recommends full disk encryption as it is easier for users.

4.2.2 Encrypting protected data in transit

As well as protecting data on devices and media, the Setting also encrypts personal data that is transmitted between systems, applications or locations (known as data in transit). Secure transmission of data relies on encryption, authorisation and authentication.

Secure transmission involves:

- encrypting the data
- making sure that computers communicating are who they say they are
- making sure that a user at the remote end is who they say they are
- ensuring that a user is authorised to access the data.

4.2.3 Securely deleting protected data

A normally deleted file can be recovered, since only the directory entry and not the file contents are removed from the disk. Government guidelines mandate the secure deletion of files (when they are no longer needed) by randomly overwriting files to government standards (usually seven times).

4.3 Audit logging and incident handling

Audit logging is only valuable if organisations collect the correct log data and store it securely.

HNS&CC collects data in ways that does not overburden systems or make unnecessary work for technicians.

It is a legal requirement of the Data Protection Act 1998 to have a statement of intent that tells staff what kinds of actions are logged or monitored and the level of detail involved.

4.3.1 Audit logging

HNS&CC collects and logs data from a range of items including physical devices, network and security devices, hosts, databases, and commercial and bespoke applications. Log collection infrastructures secure log data and collect data of evidential quality.

where appropriate, the Setting ensures that the logging infrastructure and policies are aligned with the local authority and network service provider.

HNS&CC retains logs for the length of time stated in the retention policy. The duration depends on the systems being monitored and the type of data involved

The first steps to implement an infrastructure include:

- listing critical systems (including those with sensitive and personal data) and determining what logging is turned on, where this log data is stored, how long it needs to be kept, the format, who owns the system and who can access it
- calculating the amount of data produced to work out network bandwidth and storage space requirements and recording format
- getting hold of the necessary servers, hubs, network attached storage and firewalls to build a secure internal area for these items
- named staff who have responsibility for operating the infrastructure (including the information that is to be reported), archiving processes, and procedures for resolving discoveries and remediation requirements.

4.3.2 Responding to security incidents

Data Handling Procedures in Government requires the Setting to have in place a process for responding to security incidents.

Organisations need to know that a security incident has happened before they can respond. The sooner an organisation contains an incident, the lower the risk of harm to individuals or the organisation through financial or reputation loss or data compromise.

The following points are key to managing incidents:

- Management commitment, in human resources, budget and priority
- A resolution team

- A person who is primarily responsible for each incident
- A communications plan, including escalation procedures
- Plan of action for rapid resolution
- Plan of action for non-recurrence
- Knowledge base of past security incidents, including steps taken for resolution and non-recurrence
- An awareness campaign.

4.4 Secure remote access

The Setting strives to reduce the need for two-factor authentication by choosing the kind of data that users can access remotely with care. This is particularly important for putting in place online reporting to parents, who do not need to use two-factor authentication.

5 Quick wins for data handling compliance

HNS&CC recognises that conflicts exist in existing policy, practice, technology and budgets. The Setting recognises there are a number of requirements that organisations can implement more easily to reduce the risks of security incidents.

5.1 Operational

- Make sure staff with access to personal data on children or vulnerable adults have enhanced Criminal Records Bureau (eCRB) clearance.
- Appoint a Senior Risk Information Officer (SIRO).
- Identify information assets and for each one, identify an Information Asset Owner.
- Conduct data security training for all users.
- Put in place a policy for reporting, managing and recovering from incidents which put information at risk.
- Shred, pulp or incinerate paper when no longer required.
- Make staff and learners (and parents where applicable) aware of what data is being held about them and what it is being used for by issuing privacy or fair processing notices
- Make sure that, where appropriate, contracts for employment state that misuse of such data is a disciplinary matter.

5.2 Technological

- Implement two-factor authentication for all users with access to large data sets, such as all the contents of a management information system.
- Implement and/or require suppliers or hosting partners to implement SSL or IPSec encryption for remote access to personal data in management information systems, learning platforms and portals.

- Encrypt media that contains personal data that is to be removed from the organisation.
- Securely delete and overwrite to government standards all files that contain personal data when no longer required.

6 Additional requirements

HNS&CC supports the following steps

- Incorporate requirements for managing information risk in HR and contract processes as necessary.
- Ensure all new or changed contracts implement the latest Office of Government Commerce (OGC) security and data protection clauses.
- Conduct privacy impact assessments in accordance with the ICO
- Report significant data protection incidents through the SIRO to the ICO based on the local incident handling policy and communication plan.

6.1 Technological

- Stipulate that suppliers implement encryption and remote access requirements in each application.
- Require suppliers to implement protective markings for any system-printed material that contains personal or sensitive data.
- Put in place an audit logging infrastructure.
- Implement necessary changes to applications to restrict access.