HADLEIGH INFANT & NURSERY SCHOOL

Security Measures Procedures

2022 – 2023

Version	3
Document authors	Lucy Fynn
Other contributors	**IGS**
Procedures produced (date)	September 2023
Procedures to be reviewed (date)	September 2024
Other related policies	**Data Protection Policy** **Data Handling Security Policy** **Security Incident Policy** **Complaints Policy** **Procedures for Reporting and Handling Security Incidents Policy** **Whistle-blowing Policy**

Version History Log for this document

Version	Date Published	Details of key changes from previous version

3	Sept 2023	Siro and Data Governor name change.
2	December 2021	Additional comments added to Section 2-a-ii - firewalls. Additional commented added to Section 2-a-viii - Penetration Testing.
1	August 2019	New policy created

1. Organisational

a. Policies & Documented Procedures

Policies relating to information governance issues are drafted by employees with detailed knowledge of legal requirements and the Organisation's processes. All policies have documented review dates and ownership is assigned. Reviews are held ahead of the expiry date or sooner where there is an identified issue. All policies follow a governance route for approval. Key policies are published to the organisation's website for transparency.

b. Roles

The organisation has a named Data Protection Officer who is Ms. L. Almond. This Officer executes the role by reporting the outcome of statutory process to Mrs L Fynn who acts as the organisation's Senior Information Risk Owner. Mrs. A. Cain, Information Champion, works alongside the SIRO in the school setting. Mr C Evans is the school's Information Governor.

c. Training

The organisation regularly reviews our employee roles to ensure that training and awareness messages are appropriate to the nature and sensitivity of the data processing undertaken. Induction processes ensure new employees receive appropriate training

before accessing personal data, and all other employees receive refresher training annually. All training received is documented for evidence purposes.

d. Risk Management & Privacy by Design

The organisation identifies information compliance risks on its risk register. Risks are assigned clear ownership, rated against a consistent schema; appropriate mitigations are identified and are annually reviewed.

e. Contractual Controls

All Data Processors handling personal data on behalf of the organisations have given assurances about the compliance of their processes; either through procurement assurances/ evidence, contractual agreement controls, risk assessments or supplementary statements.

f. Physical Security

All employees or contractors who have access to our premises where personal data is processed are provided with Identity Cards/Visitors' badges which validate their entitlement to access. The organisation operates processes which ensure only those individuals who have an entitlement to access premises are able to. Access to physical storage holding sensitive personal data is further restricted either through lockable equipment with key or code control procedures or through auditable access to specific rooms/ areas of buildings.

g. Security Incident Management

The organisation maintains a security incident process (Security Incident Policy) which, with the support of appropriate training, defines what constitutes a breach of these security measures to facilitate reporting of incidents. The process covers investigation of incidents, risk rating and decisions over whether to notify an incident to the Information Commissioner's Office (ICO) within the statutory timescale. Incidents are reported to the

school's SIRO (Mr. S. Proctor) or the IC (Mrs. A. Cain) and actions are consistently taken and lessons learned implemented.

2. Technical

a. Data at Rest

i. Use of Hosting Services

Some personal data is processed externally to the organisation's managed environment by third parties in data centres under agreed terms and conditions which evidence appropriate security measures.

ii. Firewalls

Access to the Organisation's managed environment is protected by maintained firewalls. Business needs to provide access through the firewall go through a strictly documented change control process which include risk assessment and approval.

iii. Administrator Rights

Enhanced privileges associated with administrator accounts are strictly managed. Members of the Senior Leadership Team and key administrative staff are the only personnel that have access to the administrator accounts (SIMS/Admin Server).

iv. Access Controls

Access permissions to personal data held on IT systems is managed through role based permissions. Managers of appropriate seniority inform IT professionals of additions, amendments and discontinuation of individual accounts within permission groups. Managers are periodically required to confirm that current permissions for which they are the authoriser and employees associated with these permissions are accurate.

v. Password Management

The organisation requires a mandatory password complexity combination of minimum length and characters (at least 10 characters and must include at least one capital, number and symbol), plus a required **change of password after each half term** (approximately 70 days).

vi. Anti-Malware & Patching

The organisation IT support assistant promptly implements any security updates provided by the suppliers of active software products.

vii. Disaster Recovery & Business Continuity

As part of the organisation's business continuity plan, there is provision to ensure effective processes are in place to both safeguard personal data during a service outage incident and to re-establish secure access to the data to support data subject rights in ongoing service provision. The business continuity plan is reviewed and updated on an annual basis. A hard copy, of the plan, is kept off site. A further two copies of the plan are kept on separate encrypted memory sticks. One is located in the school safe and the second is kept securely off-site (Junior School).A final version is kept on the school's OneDrive business area.

viii. Penetration Testing

Monthly penetration test is carried out to identify any weaknesses and potential areas of exploitation to maximise the security of the data we hold.

b. Data in Transit

i. Secure email

The organisation has access to secure email (egressswitch) software for communicating with some third parties where licensing agreements permit this. Sensitive data will be sent using such tools where available. Where software is not available a system of password protecting sensitive data in email attachments is employed.

ii. Secure Websites

The organisation has access to third party websites which allow for secure upload of personal data (NCA tools). The organisation uses these facilities to fulfil statutory obligations to report personal data to other public authorities.

iii. Encrypted Hardware

Devices which store or provide access to personal data are secured by password access*. Documents that include personal data are secured by password access.

* Passwords, for devices, are updated in line with the guidance set out in the paragraph 2.a.v within this document.

iv. Hard-Copy Data

The removal of personal data in hard-copy form is controlled by organisational policy (Data Handling Security Policy) which outlines for employees the steps that they must take to conceal the data and appropriately secure the data during transport.

These security measures are reviewed annually and approved as accurate and appropriate by the organisation's governance process.