



Holly Hill Primary School

SECURITY MEASURES (H2)

Approved by	Holly Hill Primary School Governing Body
Date Approved	Approved 20.05.2026
Version	Version 10 (FW2022)
Review Date	May 2027

An outline of the Organisational and Technical Security measures deemed appropriate by the Data Controller for the nature of the personal data processed by the Controller and any Data Processor acting on its behalf

Description of Security Measures employed to safeguard the processing of Personal Data

1. Organisational

a. Policies & Documented Procedures

Policies relating to information governance issues are based on the templates from NCC /IGS Essex County Council and adjusted by employees with detailed knowledge of legal requirements and the Organisation's processes. All policies have documented review dates or date checked dates and approved or adopted by the School Governing Body. Reviews are held ahead of the expiry date or sooner where there is an identified issue. Key policies are published to the organisation's website for transparency.

b. Roles

The organisation has a named Data Protection Officer who is Mrs. Sharon Seery. This Officer executes the role by reporting the outcome of statutory process to Mrs. Leanne Steed who acts as the organisation's Senior Information Risk Owner.

(Information on roles ref documents [A1, A6](#))

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. ([link to D10, B1](#))

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. ([link to documents in section G](#))

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. ([link to documents in section E and G](#))

f. Physical Security

All employees or contractors who have access to our premises where personal data is processed are provided with Identity Cards or visitor 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 or doors with key or code control procedures to specific rooms/ areas of buildings. [\(link to documents in section C and D\)](#)

g. Security Incident Management

The organisation maintains a security incident process 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 senior leaders and actions are consistently taken and lessons learned implemented. [\(link to documents in section C and D\)](#)

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 and compliance with the law.

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. (ATOM IT)

iii. Administrator Rights

Enhanced privileges associated with administrator accounts are strictly managed. Administrator activities are logged by the inbuilt log within the online / cloud system being used to ensure activity can be effectively monitored as required.

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. Elimination of weak passwords system setting has been activated.

Multi-factor authentication enabled on staff accounts.

Certain secure web sites and Cloud based services request frequent updates to password management and provide prompts to changes.

vi. Anti-Malware & Patching

The organisation uses Cynet for antimalware and antivirus. (ATOM IT) Patching of Windows is automatically done. (ATOM IT)

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.

Redstor back-up is used to support disaster recovery. (ATOM IT)

viii. Penetration Testing / Vulnerability scanning

Multi-factor authentication and VPN use with domain credentials support to reduce vulnerability of the network.

Our broadband connections have vulnerability scanning in place to detect and protect our network. (ATOM IT)

b. Data in Transit

i. Secure email

The organisation has access to secure email 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 or email encryption is employed.

ii. Secure Websites

The organisation has access to third party websites which allow for secure upload of personal data. 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. (Working towards removable media such as memory sticks are encrypted or reduced use or cloud-based storage)

iv. Hard-Copy Data

The removal of personal data in hard-copy form is controlled by organisational policy which requires employees to take steps 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.