Information Governance Support

Essex County Council

Approved by	Melissa Mulgrew
Date Approved	07/07/2021
Version	1.0
Review Date	07/07/2022

SECURITY MEASURES

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 Processors 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 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.
   Procedures are documented by subject matter experts and approved by line managers, with regular review dates appropriate to the procedure documented.

   b. Roles

   The organisation has a named Data Protection Officer who is Lauri Almond, of Essex County Council Information Governance Service This Officer executes the role by reporting the outcome of statutory process to Nicole Chapman (Headteacher) who acts as the organisation's Senior Information Risk Owner. Day to day management of information security issues is delegated to Melissa Mulgrew, Business Manager, on behalf of the SIRO.

   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 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 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.

2. Technical

a. Data at Rest

i. Use of Hosting Services

- Office 365 (staff and student email) – data stored in Europe
- Parentpay – Held in EEA
- SIMS Parent App
- Evolve / Wonde

Where Microsoft Online Services stores customer content

Service	Data at Rest
Exchange	Europe
SharePoint	Europe
Skype for Business	Europe
Microsoft Teams	United Kingdom

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

- Smoothwall Firewall
- Windows firewall (ports blocked unless needed)

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

- IT staff don't have admin rights by default.
- Appropriate documented accounts have admin rights. Mostly Service accounts.

Enhanced privileges associated with administrator accounts are strictly managed. Administrator activities are logged and auditable to ensure activity can be effectively monitored.

iv. Access Controls

- Security rights on folder shares (based on users and groups)
  - Mainly based on subject areas folders on the R drive, and U drive access.

- SIMS permissions - users can only get to areas they need to
  - Sims permissions reviewed on a regular basis

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

- Required change every 90 days
- Complex Passwords required
- Minimum 6 characters

The organisation requires a mandatory password complexity combination of minimum length and characters, plus a required change of password after 90 days.

vi. Anti-Malware & Patching

- Avast Antivirus
- Auto-updates virus definitions in line with Avast releases
- On demand scanning of files
- Client machines are patched as soon as patches have been released and tested.
- Servers are patching during the holidays, or after two weeks from a patch being made available, whichever is the soonest. Arranged by IT Manager.

The organisation has a documented change control process which facilitates the prompt implementation of any security updates provided by the suppliers of active software products.

vii. Disaster Recovery & Business Continuity

- DR testing every holiday, where possible – results documented and stored on network share.
  - Enable servers to be restored in DR room in event of server room failure.
- Email system cloud based. Allows continued communication with students and parents.

igs

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.

b. Data in Transit

    i. Secure email

- Egress installed on select user machines where personal data is being exchanged (e.g. Payroll, SENCO).
- Egress not 100% free, so not installed sitewide.
- Where the above is not possible, files are password protected, and password sent in a separate 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 in email attachments is employed.

    ii. Secure Websites

- Parentpay
- SIMS Parent App
- Evolve / Wonde
- Groupcall xporter for sending information to ECC

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

- Offline X drives on staff laptops encrypted.
- No removable storage allowed.
  - Account set up for external visitors with just removable storage access – need to confirm it is clean before being allowed use.
  - Super users have access (IT staff, Exams during exam period)

Devices which store or provide access to personal data are secured by password access. Removable media such as memory sticks are only allowed by exceptional approval and are otherwise blocked.

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.

Printing from the school's systems to home devices is blocked.

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