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 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 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 Lauri Almond. This Officer executes the role by reporting the outcome of statutory process to Lorraine Ramet who acts as the organisation's Senior Information Risk Owner.

    The school has a Data Protection Lead Juliet Archer who ensures the school complies with all data protection policies and procedures and manages the administration of data protection matters, reporting to 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 school are subject to contractual obligations or other legally binding agreements.

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

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

LgFL provide all the firewall protections as well as many other layers of defence.

iii. Administrator Rights

Administration rights are maintained by our IT Support Company ITHelpDirect Ltd. They have strict logging, training and monitoring for their employees.

iv. Access Controls

Certain information is restricted for difference staffing levels, e.g. Finances, Student Databases etc.
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 school requires a mandatory password complexity combination of minimum length and characters.

vi. Anti-Malware & Patching

The school has a site wide license for Sophos which includes the antivirus and intercept x options

vii. Disaster Recovery & Business Continuity

The disaster recovery solution in place is an onsite NAS followed by offsite backup of encrypted Virtual Machines for quick restore, this is done daily. Also in line with continuity we backup each user's files through a cloud system that backs up every hour including incremental changes and deletion retention for 60 days.

viii. Penetration Testing / Vulnerability scanning

We run penetration tests via LgFL once a year to confirm any exploits or issues that arise from the report, followed by a fix of these then a rescan to confirm.

b. Data in Transit

i. Secure email

Email is mainly through Microsoft 365 but when sensitive documents are required they are password protected and details given to the relevant person over the phone to access.

ii. Secure Websites

Local authorities provide us with secure FTP or secure areas to upload data.

iii. Encrypted Hardware

All laptops where they are taken offsite have Bitlocker encryption enabled.

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.