Bracken Hill School

Security Measures Policy and Procedure

Author: Mrs Austin

Policy Type: Whole School

This policy is reviewed biennially to ensure compliance with current regulations

SECURITY MEASURES POLICY AND PROCEDURE

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.

    b. Roles

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

    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 scheme, 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

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.

The services we use are Microsoft Office 365 for emails which are UK based and our data back-up is facilitated by Atom IT who are again based in the UK.

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.

Data in school is protected by Fortinet which is maintained by both the ICT Technician and Atom IT. The internet is governed by Fortinet's web filter which is updated and monitored weekly. End users are protected by Avast Anti-virus.

iii. Administrator Rights

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

Administrator rights are used only by the ICT manager, the ICT coordinator, the ICT Technician and support from Atom IT. The school hosts a structured system with regards to user rights where teachers, the office administrators and SLT have tailored rights but not those of an administrator.

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

We require a mandatory password complexity combination of upper case letters, lower case letters and a number. Passwords should be changed every 90 days.

vi. Anti-Malware & Patching

The organisation has a documented change control process which facilitates the prompt implementation of any security updates via Fortinet or Avast. This protects from any outside threat.

vii. Disaster Recovery & Business Continuity

The school has both an on-site backup in case of a data disaster and an off-site backup with Atom IT in case of fire or theft. This will maintain business continuity in the event of disaster recovery.

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 in email attachments is employed.

The schools emails are hosted by Microsoft 365. This is coupled with the new function called Azure Data Protection. If this is ever unavailable then documents are password protected before sending.

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.

The third party websites used in school are accredited websites including Behaviour Watch and Solar and Crypto Share in association with Notinghamshire County Council.

iii. Encrypted Hardware

Devices which store or provide access to personal data are secured by password access. Removable media such as memory sticks are encrypted.

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. The school uses a shredding service to ensure that all hard copy data is destroyed effectively at the appropriate time.

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