Eastwood Park Academy Trust (EPAT)

EPAT

Believe Succeed Together

Description of Security Measures Employed to Safeguard the Processing of Personal Data

Date Reviewed	June 2022
Date Ratified by Trust	July 2022

Contents

1.0 Organisational 2
1.1 Policies and Documented Procedures 2
1.2 Role 2
1.3 Training 2
1.4 Risk Management and Privacy by Design 2
1.5 Contractual controls 2
1.6 Physical Security 2
1.7 Security Incident Management 2
2.0 Technical 3
2.1 Data at Rest 3
2.11 Use of Hosting Services 3
2.12 Firewalls 3
2.13 Administrator Rights 3
2.14 Access Controls 3
2.15 Password Management 3
2.2 Data in Transit 4
2.21 Secure E-mail 4
2.22 Secure Websites 4
2.23 Encrypted Hardware 4
2.24 Hard-Copy Data 4

1.0 Organisational

1.1 Policies and Documented Procedures

Policies relating to information governance issues are drafted by employees with detailed knowledge of legal requirements and the Trust's processes. All policies are reviewed annually or sooner where there is an identified issue. All policies are approved by Trustees and are published on the Trust's website.

1.2 Role

The organisation has a named Data Protection Officer (DPO) - **Lauri Almond**. The DPO executes the role by reporting the outcome of statutory process to the Trust's Senior Information Risk Owner (SIRO) - **Mr. Neil Houchen.**

1.3 Training

The Trust regularly reviews its 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.

1.4 Risk Management and Privacy by Design

The Trust 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.

1.5 Contractual controls

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

1.6 Physical Security

All employees or contractors who have access to the premises of a constituent academy where personal data is processed, are provided with identity cards which validate their entitlement to access. The Trust 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.

1.7 Security Incident Management

The Trust 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.

2.0 Technical

2.1 Data at Rest

2.11 Use of Hosting Services

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

2.12 Firewalls

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

2.13 Administrator Rights

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

2.14 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.

2.15 Password Management

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

2.16 Anti-Malware and Patching

Microsoft Windows update manages Trust devices unless there is a third party software 'patch'.

The Trust use Sophos which monitors all devices connected to the network and removes any anti-malware.

2.17 Disaster Recovery and Business Continuity

As part of the Trust'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 using Symantec backup, exec to tape, and also backup assist which backs data to a physical server.

2.2 Data in Transit

2.21 Secure E-mail

The Trust 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 passwords protecting sensitive data in email attachments is employed.

2.22 Secure Websites

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

2.23 Encrypted Hardware

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

2.24 Hard-Copy Data

In terms of the removal of personal data in a hard-copy form, employees are required to take steps to conceal and appropriately secure the data during transport – refer to the Employee Code of Conduct Policy.