Blackpool Skills Academy – Data Security Policy

1. Purpose

Blackpool Skills Academy (BSA) is committed to protecting the confidentiality, integrity, and availability of all personal and organisational data. This policy sets out how data is secured, managed, and protected in line with UK GDPR, Data Protection Act 2018, and safeguarding requirements.

2. Scope

This policy applies to:
- All staff, governors, contractors, and volunteers handling Academy data.
- All forms of data: electronic, paper, verbal, images, and CCTV.
- All systems, including Bromcom MIS, email, HR/payroll systems, and therapy reports.

3. Roles and Responsibilities

- Data Controller: Blackpool Skills Academy.
- Data Protection Lead (DPL): Responsible for ensuring compliance and reporting breaches.
- All Staff: Must follow this policy, complete data protection training, and report incidents immediately.
- Third-Party Processors: Must comply with GDPR and have contractual agreements in place.

4. Data Security Principles

BSA will ensure:
- Confidentiality: Data is accessible only to those authorised.
- Integrity: Data is accurate, up to date, and protected from alteration.
- Availability: Data is accessible when required for operational or safeguarding purposes.

5. Technical Measures

- All Academy systems (e.g., Bromcom MIS) are password-protected, encrypted, and regularly updated.
- Strong password policies and 2-factor authentication are in place.
- Regular data backups are performed and securely stored.
- Academy devices (laptops, tablets, phones) are encrypted and tracked.
- Firewalls, antivirus, and intrusion detection systems are maintained.

6. Organisational Measures

- Staff receive annual training in data protection and cyber security.
- Role-based access ensures staff only see the data they need.
- Data minimisation: only essential personal data is collected and retained.
- Regular audits of data processing and security arrangements are carried out.

- Contractors, visitors, and external partners must comply with Academy data security requirements.

7. Physical Security

- Paper records are stored in locked cabinets and secure offices.
- Access to buildings is controlled via sign-in, ID badges, and CCTV monitoring.
- Visitors are supervised at all times.

8. Data Sharing and Sub-Processors

- Data is only shared where lawful and necessary (e.g., with Local Authorities, exam boards, NHS, safeguarding teams).
- Data Processing Agreements (DPAs) are in place with all processors (e.g., Bromcom, payroll providers).
- Processors must notify BSA of any sub-processors used and remain fully liable for their compliance.

9. Incident Management and Breach Reporting

- Any data breach or security incident must be reported immediately to the Data Protection Lead.
- The DPL will investigate, record, and where required notify the ICO within 72 hours.
- A log of all incidents will be maintained and reviewed by SLT.

10. Retention and Disposal

- Data is retained in line with the Academy's Retention Schedule (based on IRMS guidance).
- When no longer required, data will be securely deleted (electronic) or shredded (paper).

11. Monitoring and Review

This policy will be reviewed annually, or sooner if required by legislation or organisational change.
Compliance will be monitored through audits, incident logs, and staff feedback.

Signed: 

Headteacher / Data Protection

Lead Date: 26/09/26