



Cyber Security Policy 25/26

We do things differently.....

H.E.R.E

**High Standards
Empathy
Resilience
Emotional Response**

Contents

1. Statement of Intent	2
2. Legal and Regulatory Framework	3
3. Roles and Responsibilities.....	3
3.1 Governing Body.....	3
3.2 Headteacher.....	3
3.3 Data Protection Officer (DPO)	3
3.4 All Staff.....	4
4. Technical and Organisational Security Measures	4
Access Controls	4
Network Security	4
Data Protection Controls	4
Malware Protection	4
Physical Security	4
5. Lawful Monitoring.....	5
6. Definition of a Personal Data Breach.....	5
7. Breach Reporting Procedure.....	5
7.1 Immediate Reporting.....	5
7.2 Risk Assessment.....	5
8. ICO Notification (Article 33 UK GDPR)	5
9. Communication with Individuals (Article 34 UK GDPR).....	6
10. Personal Data Breach Register.....	6
11. Third Party Notification.....	6
12. Training and Review.....	6
13. Policy Review	7

1. Statement of Intent

The Kassia Academy is committed to ensuring the confidentiality, integrity and availability of its information systems and personal data. The school recognises its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and associated legislation to protect personal data and maintain effective cyber security arrangements.

The school will implement appropriate technical and organisational measures in accordance with Article 32 UK GDPR to ensure a level of security appropriate to the risk, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The school acknowledges that security incidents and personal data breaches may occur despite preventative measures. Where this happens, the school will:

- Respond promptly and proportionately;
- Mitigate risks to individuals;
- Comply with statutory reporting obligations;

- Maintain a documented breach record;
- Take action to prevent recurrence.

This policy applies to all staff, governors, contractors, volunteers and third parties processing data on behalf of the school.

2. Legal and Regulatory Framework

This policy has due regard to the following:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Computer Misuse Act 1990
- Privacy and Electronic Communications Regulations (PECR) 2003
- Human Rights Act 1998 (Article 8 – Right to Privacy)
- Network and Information Systems Regulations 2018 (where applicable)
- ICO Guide to the UK GDPR
- ICO Personal Data Breach Guidance
- DfE Cyber Security Standards for Schools and Colleges
- DfE Meeting Digital and Technology Standards in Schools and Colleges
- ESFA Academy Trust Handbook
- NCSC Cyber Essentials Guidance

This policy operates alongside:

- Data Protection Policy
- Online Safety Policy
- Acceptable Use Policy
- Staff Privacy Notice
- Behaviour Policy
- Disciplinary Policy

3. Roles and Responsibilities

3.1 Governing Body

The Governing Body has overall accountability for ensuring compliance with data protection and cyber security legislation.

3.2 Headteacher

The Headteacher is responsible for operational management of cyber security arrangements and incident response.

3.3 Data Protection Officer (DPO)

The appointed Data Protection Officer will:

- Be informed immediately of any suspected or confirmed personal data breach;
- Advise on breach risk assessment;

- Determine whether ICO notification is required;
- Oversee communication with affected individuals;
- Maintain the Personal Data Breach Register;
- Monitor compliance with UK GDPR.

The DPO operates independently in accordance with Article 38 UK GDPR.

3.4 All Staff

All staff must:

- Follow security and acceptable use procedures;
- Report suspected data breaches immediately;
- Complete mandatory training;
- Safeguard personal data appropriately.

Failure to comply may result in disciplinary action.

4. Technical and Organisational Security Measures

In accordance with Article 32 UK GDPR, the school implements measures including:

Access Controls

- Role-based access control
- Access Control Lists (ACLs)
- Multi-Factor Authentication (MFA), particularly for administrative accounts
- Strong password standards

Network Security

- Firewalls and Next-Generation Firewalls
- Web Application Firewall (WAF)
- Network monitoring and intrusion detection
- Regular vulnerability scanning
- Secure port configuration

Data Protection Controls

- Encryption of devices and portable media
- Secure VPN connections using industry-standard encryption
- Offline and secure backup systems
- Patch management procedures
- Supported operating systems only

Malware Protection

- Anti-virus and anti-malware software
- Heuristic threat detection
- Email filtering and phishing protection

Physical Security

- Secure storage and locking of equipment

- Controlled site access
- Asset management procedures

5. Lawful Monitoring

Any monitoring of staff devices or network usage will:

- Be lawful, fair and transparent;
- Be proportionate and necessary;
- Be outlined in the Staff Privacy Notice;
- Have a lawful basis under Article 6 UK GDPR;
- Where applicable, meet Article 9 UK GDPR requirements for special category data.

Monitoring will respect individuals' rights under the Human Rights Act 1998.

6. Definition of a Personal Data Breach

Under Article 4(12) UK GDPR, a personal data breach is:

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes loss, theft, hacking, accidental disclosure, ransomware or unauthorised access.

7. Breach Reporting Procedure

7.1 Immediate Reporting

All suspected breaches must be reported immediately to:

- The Headteacher
- The Data Protection Officer

7.2 Risk Assessment

The Headteacher and DPO will assess:

- Nature and volume of data involved
- Sensitivity of data
- Number and type of individuals affected
- Likely consequences
- Protective measures in place
- Risk to rights and freedoms

Risk considerations include physical safety, emotional wellbeing, identity theft, financial loss and reputational harm.

8. ICO Notification (Article 33 UK GDPR)

Where a breach is likely to result in a risk to individuals' rights and freedoms, the school will notify the Information Commissioner's Office:

- Without undue delay; and
- Where feasible, within 72 hours of becoming aware of it.

If notification is delayed, reasons will be documented.

Where the breach is not reported, the rationale will be recorded in the Personal Data Breach Register.

9. Communication with Individuals (Article 34 UK GDPR)

Where a breach is likely to result in a high risk to individuals, affected individuals will be informed without undue delay.

Notifications will include:

- Description of the breach
- Likely consequences
- Steps taken to mitigate risk
- Advice on protective measures
- DPO contact details
- Right to complain to the ICO

10. Personal Data Breach Register

In accordance with Article 33(5) UK GDPR, the school will maintain a Personal Data Breach Register documenting:

- Facts relating to the breach
- Effects of the breach
- Remedial actions taken
- ICO reporting decisions

All breaches will be recorded, regardless of severity.

11. Third Party Notification

Where appropriate, the school may notify:

- The Trust
- ESFA
- Police
- Insurers
- System providers
- Banks or other affected organisations

12. Training and Review

The school will:

- Provide annual data protection and cyber security training;
- Conduct periodic awareness exercises;
- Review cyber risks annually;
- Align practice with DfE Cyber Security Standards;
- Embed Cyber Essentials principles.

13. Policy Review

This policy will be reviewed annually or sooner if:

- Legislation changes;
- ICO guidance is updated;
- A significant breach occurs.

DRAFT