Data Protection Policy

Policy statement

1. The Acer Trust is committed to respecting and safeguarding the privacy of our pupils, students, staff, families and all other stakeholders. Therefore, we will take all reasonable steps to protect the security and integrity of our data, in line with relevant legislation and best practice guidance.

Scope

2. This policy outlines our approach to data protection and our responsibilities towards this; it applies to all information systems, software and physical records, and to all who have access to them. The policy complies with our obligations under the Data Protection Act (2018), Education (Pupil Information) (England) Regulations 2005 and our funding agreements.

Responsibilities

3. As users of school and Trust systems, and processors of personal data, we are all responsible for:
   - protecting the information we handle and following relevant policies and processes;
   - respecting the boundaries identified in relevant policies, procedures and guidance;
   - remaining vigilant to data security threats, including cyber-attacks.

4. The Trust Data Protection Group is responsible for:
   - Taking a collective view of data protection across the Trust;
   - Collaborating to drive improvements in data protection practice;
   - Monitoring data protection related risks and recommending action.

5. School Data Protection Leads are responsible for:
   - Participating in the Trust Data Protection Group;
   - Promoting and supporting data protection best practice;
   - Providing advice and guidance or escalating queries relating to data protection;
   - Coordinating responses to data breaches and rights requests.

6. Headteachers are responsible for:
   - Appointing a Data Protection Lead for the school;
   - Ensuring that staff are aware of and follow this policy and relevant procedures and guidance;
   - Ensuring that data protection related records and paperwork is completed and up to date.

7. School Governing Bodies are responsible for:
   - Adopting robust data protection policies and procedures;

- Ensuring, through school leadership, that the school complies with its obligations in respect of data protection.

8. The Data Protection Officer (DPO) is responsible for:
   - providing advice, guidance and training about data protection;
   - monitoring compliance with relevant guidelines and maintaining central records.

9. Acer Trust is the registered Data Controller for all personal data processed within the Trust and its partner schools. The Trust fulfils its duties through this policy and the work of the DPO and school leaders.

Data Protection Core Principles

10. We are committed to the principles of data protection:
    - **Lawful, fair and transparent processing:** We only process personal information where:
      - we have a lawful basis to do so;
      - it is considered fair to the subject of the information; and
      - they have been informed about it (usually through Privacy Notices).
    - **Purpose limitation and data minimisation**: We are clear about the purpose for collecting personal information and only use it for compatible purposes. We avoid duplication of information by using central databases and cloud sharing facilities where possible.
    - **Accuracy:** We are committed to keeping information accurate and up to date and promptly correcting erroneous data.
    - **Storage limitation:** We store information in a secure and orderly way, so that we keep it no longer than is necessary.
    - **Security, integrity and confidentiality:** We make sure that our information and systems are safe from misuse by following IT guidelines. We will all:
      - use only secure devices to access school and Trust information and systems;
      - refrain from storing personal information on USB devices;
      - manage passwords and account access securely;
      - only use authorised email and storage accounts to access, store, or share information;
      - make proper use of secure digital and physical storage solutions;
      - maintain a clear-desk policy and secure records when not in use;
      - share information securely; and
      - dispose of information securely, such as through the confidential waste facilities provided.
    - **Transfer limitation:** We recognise that some countries may not provide the same standard of data protection. Because of this, we do not transfer information outside the European Economic Area without due care and the approval of the DPO.
    - **Data subjects' rights and requests:** We recognise people's data rights, including:
      - the right to request access to data;
      - erasure or rectification of data; or
      - the right to request information about the data we hold about them.

      We all look out for such requests and report them immediately to the school Data Protection Lead.
    - **Privacy by design:** We seek to find creative, efficient and effective solutions that reflect the principles of data protection and information security. All new data processes are subject to a Data Protection Impact Assessment.

Automated Processing and Automated Decision-Making

11. Before we undertake automated processing or decision-making, we will conduct a Data Protection Impact Assessment and seek the approval of the DPO.

Direct Marketing

12. We only promote our services in ways that respect people's privacy and comply with the law.

Freedom of Information

13. As a public authority, we publish certain information online and process requests for information promptly. We all remain vigilant to requests made under the Freedom of Information Act and report them immediately to the relevant staff member.

Record Keeping

14. We keep robust records of our data processing activities. Where we process information based on consent, we keep records of this.

Training, Audit and Governance

15. We ensure that we provide access to data protection and information security training, including annual onlinetraining. Our school Data Protection Leads receive additional training and provide support and guidance to their schools. We carry out internal audits regularly to identify best practice and areas for improvement.

Breaches of data security

16. We respond quickly and comprehensively to breaches in data security to minimise the impact on the Acer Trust and any people affected. We remain vigilant to potential breaches and report them via GDPRiS immediately. We report high risk to the Information Commissioner's Office and/or data subjects as appropriate. We may follow up failure to report breaches to ensure staff fully understand the importance of reporting, including disciplinary action where necessary.