

## **Data Protection Policy**

*Approved by the Board of Trustees, 15 July 2015.*

The Greenshaw Learning Trust recognises and accepts its responsibility as set out in the Data Protection Act 1998 and sub-legislation contained therein. The Trust, as a Data Controller, will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information. In particular the Trust and the schools within it will comply with the Data Protection Principles set out in the 1998 Act.

This policy statement applies to the Trust and all schools within it, and to all employees, students, Trustees and governors and other individuals about whom the Trust and its schools process personal information, as well as other partners and companies with which the Trust undertakes its business.

### **Personal Data**

All personal data is to be managed in accordance with the Data Protection Act 1998. The Trust is a Data Controller for the purposes of the Act and has registered with the Information Commissioner.

The Trust processes personal data for these purposes:

- Education
- Educational Support and ancillary purposes
- School administration
- Staff, agent and contractor administration
- Advertising Marketing, public relations, general advice

This data protection policy covers personal data collected for the above purposes whoever the personal data belongs to.

Data is 'personal data' if it relates to an individual and the individual can be identified from that data. It is caught by the act if it is filed, electronically stored or processed.

### **Sensitive personal data**

This is information about an individual's:

- Race/ ethnicity
- Religious beliefs or those of a similar nature
- Political views
- Trade Union membership
- Physical or mental health
- Sexual life/orientation
- Commission or alleged commission of any offence or any related court proceedings

### **Management of Data**

The Trust is responsible for making sure that personal data is managed in accordance with the Data Protection Act. The day to day management of this is designated to Trust's Head of

Resources but all staff of the Trust and its schools are responsible for ensuring that they read this policy and comply with it and the Data Protection Act 1998. Where a member of staff has particular responsibility for data compliance, they should make sure they understand their role. Staff are made aware that knowingly or recklessly disclosing personal data may be a criminal offence and that internal disciplinary procedures will be followed if a member of staff commits a data breach.

The Trust will:

- Seek to ensure that no personal data is collected unless it is necessary.
- Make sure that appropriate procedures and checks are in place to ensure compliance.
- Evaluate the efficacy of the above procedures
- Ensure that explicit consent is given to any collection of sensitive personal data
- Ensure that the Trust's notification to the ICO is kept up to date.
- Make sure that personal data in manual files is stored securely in locked filing cabinets with access restricted to designated members of staff and that electronically held personal data is stored securely, again with access restricted to designated members of staff
- Send a letter to employees each year informing them of the data held about them, including the type of data, where it came from, who has access to it and why it is held. They will also be informed of their right to access the data and correct any inaccuracies

### **Disclosure of data**

Personal data will only be disclosed to third parties in two circumstances:

- Where the data subject has given consent (or in the case of a child without capacity under the Data Protection Act - ordinarily those under 12 years of age - their parent or guardian).
- Where the Trust is required or permitted by law to disclose it.

The Trust will take reasonable steps to confirm the identity of a third party requesting personal data.

Where a person wishes to access their own data, they must make a request in writing. The Trust's Head of Resources will check the identity of the requester and respond within 40 days. The request may be refused in whole or in part if the Trust has legal grounds not to comply with the request in full. Where a request is turned down reasons for the refusal will be given.

### **Recruitment**

It will be necessary for the Trust to collect information from candidates applying for a position within the Trust or any of its schools. The application form will ask for information relevant to the position applied for and the applicant's explicit consent obtained, both for the data revealed by them and for any request which will be submitted to a third party for personal data about the applicant. The applicant will be informed of:

- Why the Trust collects the information
- How long it will be kept
- The security in place to protect the information
- How the application will be processed
- How the information given will be verified