

Privacy Notice – Recruitment Candidates Data

Data Controller: Synergy Education Trust

Address: % Stanley Primary School, Wordsworth Avenue, Blackpool. FY3 9UT

Data Protection Officer: SchoolsDPO@blackpool.gov.uk

Under data protection legislation, individuals have the right to be informed about how their personal data is collected and used. This notice explains how Synergy Education Trust (“the Trust”) collects, stores and uses personal data about individuals who apply for roles within the Trust.

This privacy notice applies to all job applicants, including those applying for teaching, support, leadership, voluntary and temporary roles across the Trust.

Synergy Education Trust is the data controller for the purposes of data protection law.

Categories of Trust information that we process include:

General Personal Data

- Name, address and contact details
- Date of birth
- National Insurance number
- Right to work documentation
- Qualifications, professional memberships and training
- Employment history, references and experience
- Application forms, CVs and interview notes

Special Category Data

- Health information (including pre-employment health checks)
- Disability and access requirements
- Equality and diversity monitoring information (e.g. ethnicity, religion, sexual orientation)

Criminal Records Information

- Disclosure and Barring Service (DBS) information, including criminal convictions where relevant to the role

This list is not exhaustive, to access the current list of categories of information we process please contact the Trust office; on 01253 800318 or email: coo@seteducation.org.uk

Why we collect and use workforce information

We collect and process applicant data for the following purposes:

- To assess suitability for employment
- To make recruitment and appointment decisions
- To carry out safer recruitment and safeguarding checks
- To verify identity and right to work
- To meet legal, regulatory and safeguarding obligations
- To ensure equality, diversity and inclusion in recruitment
- To make reasonable adjustments for candidates with disabilities
- To communicate with candidates throughout the recruitment process
- To respond to complaints and defend legal claims

Our lawful basis for using the data

Under the General Data Protection Regulation (GDPR), the lawful basis bases we rely on for processing personal information for general purposes are:

- Article 6(1)(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (e.g. publication of photographs)
- Article 6(1)(b) processing is necessary for the performance of a contract with the data subject
- Article 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject; (e.g. health & safety, safeguarding)
- Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

When we collect 'special categories of personal data' e.g. Information relating to a person's racial or ethnic origin or medical information, we will do so where we have explicit consent or where it is necessary for us to comply with our obligations under employment, social security or social protection laws.

Criminal records data is processed in accordance with Article 10 UK GDPR and safeguarding legislation.

Collecting workforce information

We collect information about candidates from a variety of sources, including:

- Application forms and CVs
- Interviews and assessments
- Identity documents provided to confirm eligibility to work in the UK
- References from previous employers
- Employment agencies
- Disclosure and Barring Service
- Occupational Health providers

Most of the information we request is mandatory. Where information is voluntary, we will make this clear at the point of collection.

Storing workforce information

Applicant data is stored securely in both electronic and paper formats.

We retain personal data in line with the Trust's Data Retention Schedule, including:

- Unsuccessful applicants: normally retained for up to 6 months after recruitment
- Successful applicants: data becomes part of the employee personnel file

Where appropriate, information may be anonymised for statistical and monitoring purposes.

Who we share workforce information with

We do not share applicant data unnecessarily. Where lawful and appropriate, we may share information with:

- Members of the recruitment and interview panel
- Human Resources providers
- Disclosure and Barring Service
- Occupational Health providers
- Regulatory or safeguarding bodies where required by law

We do not sell or trade personal data.

Data Security

We use appropriate technical and organisational measures to protect personal data against loss, misuse, unauthorised access or disclosure.

Access to personal data is restricted to those who need it for legitimate purposes, and all staff are trained in data protection and confidentiality.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold.

Under data protection law, you have the right to:

- Request access to your personal data
- Request rectification of inaccurate data
- Request erasure of data (in certain circumstances)
- Restrict or object to processing (in certain circumstances)
- Withdraw consent where processing relies on consent
- Lodge a complaint with the Information Commissioner's Office (ICO)

Further information is available at: <https://ico.org.uk>

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>