Western Road Community Primary School
Privacy Notice for Staff, Trustees and Volunteers (Workforce)

Introduction

The General Data Protection Regulation (GDPR) was introduced in May 2018. This Privacy Notice describes how the school gathers and processes the personal data of staff, Trustees and volunteers at the school (Workforce). The school is a 'data controller' and must comply with the Data Protection regulations.

The processing of personal information by the school is predominantly for employment purposes and the effective support of Trustees and volunteers. The processing assists in the running of the school and contributes to local and national planning.

What information is processed?

Whilst the majority of information you provide is mandatory, some of it is provided to the school on a voluntary basis. In order to comply with data protection legislation, the school will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

The categories of workforce information gathered and processed include:

- personal information (name, contact details, employee reference, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group, union membership
- contract information (job title, responsibilities and salary information)
- payroll information (tax code, timesheets, expenses, pension, sick pay, memberships)
- absence from work (number of absences and reasons)
- qualifications and recruitment information (subject qualifications, references, employment checks, interview records and references)
- medical information (GP information, health data, disabilities, allergies, workplace assessments, accident records)
- DBS registrations information
- performance management data, appraisals, disciplinary, grievance and training data
- digital footprint from use of communication and IT equipment
- next of kin name & contact details
- photographs, CCTV, video and audio recordings

In addition, Trustee data will include:

- governance details such as; role, start and end dates, including the date of resignation and governor ID
- pecuniary and non-pecuniary interests, including business interests, other governance positions and any relationships with staff or other trustees. This is required for a register of interests published on the school website
- meeting attendance data to be published on the school website
- the committees and panels that you serve on and the link area of responsibility you have
- information related to your appointment, such as a work or personal reference
- personal information provided as a biography to be published on the website

What is the information used for?

The information gathered is used to:

- keep staff, Trustees and volunteers safe
- enable staff to be paid and contractual obligations fulfilled
- support staff health and medical emergencies and record absence
- maintain the quality of workforce data in the sector
- enable effective performance management and training needs
- support the development of recruitment and retention policies
- enable accurate financial modelling and planning
- fulfil statutory obligations under legislation (the Equality Act 2010, Keeping Children Safe in Education (KCSIE), Safeguarding Vulnerable Groups Act 2006, Health and Safety at Work Act 1974, Equality Act (Gender Pay Gap Information) Regulations 2017, Education (Health Standards) (England) Regulations 2003, Immigration, Asylum and Nationality Act 2006, Immigration Act 1971, Education and Skills Act 2008

What is the legal basis for the processing?

The school processes workforce data under the following legal bases:

Contract - to meet the contractual obligations with its workforce during the recruitment process and following employment.

Legal Obligation – to record, process and share data regarding its workforce to comply with employment law. This includes the legal duty to process governance information in respect to Trustees.

Public Interest – where processing is required in the performance of a task in the public interest.

Consent – where another legal basis is not already present, consent will be requested before processing personal data. Consent may be withdrawn at any time.

How long is data held?

Workforce data is held in accordance with the school's Retention Schedule. This is normally seven years from the date of leaving employment with the school, but in some instances (such as Asbestos exposure) this may be longer when a legal basis is present.

Who is the information shared with?

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Workforce data is shared with:

- The local Authority to support the management of workforce data across the County (section 5 of the Education - Supply of Information about the School Workforce - (England) Regulations 2007 and amendments)
- The Department for Education (DfE) and regulatory bodies such as Ofsted
- Payroll and personnel service providers
- Training, catering, occupational health providers
- Professional bodies, trade unions and associations

We are required to share information about our workforce with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments. This data sharing underpins workforce policy monitoring, evaluation and links to school funding/expenditure and the assessment of educational attainment.

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use.

In addition, Trustee data is shared with:

- School auditors
- Companies House
- the Local Authority Governor's database
- the Department for Education (DfE) and regulatory bodies such as Ofsted
- Other Board members
- On our school website

Keeping your personal information safe

The school has appropriate security measures in place to prevent personal information being accidentally lost or accessed in an unauthorised way. The school limits access, via tiered levels of security access, to personal information to those individuals with a genuine need to processes it.

Those processing personal data will do so only in accordance with school policies and procedures, and subject to a duty of confidentiality.

The school has procedures in place to deal with any suspected data security breach. The school will work with its Data Protection Officer and any applicable regulator (such as the Information Commissioners' Office), in the event of a suspected data security breach.

How can I access my data?

Data protection legislation gives individuals specific rights, which include the right to access their data. The school has an Individual Rights Form that it will use to support individuals to access their information. To make a request for your personal information, please contact the school office office@westernroad.e-sussex.sch.uk

Commented [RS1]: Please add the contact details for the school

The other rights allow individuals to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- have inaccurate personal data rectified
- to restrict or erase information that no longer has a legal basis to be held

In some circumstances, where a legal reason exists, the school may decline a request by an individual about their data. In this case an explanation will be provided as to why the school is unable to support the request.

Data Protection Officer

The school has appointed an independent Data Protection Officer as its DPO. The Data Protection Officer is Roger Simmons and may be contacted via email at rsimmonsltd@gmail.com and via telephone on 07704 838512.

However, please contact the school in the first instance if you have a query regarding this Privacy Notice or how your information is used.

Further information about the Principles of GDPR, the Rights of Individuals and the legal basis for processing data is available in the school's Data Protection and Information Security Policy.