WMAT

Job Applicant Privacy Policy - (Policies)

Weydon Multi Academy Trust

Version 1

22/04/2026

Key Details

Date Accepted: 01/04/2026

Updated: 01/04/2026

Review Date: 01/04/2027

School name: Weydon Multi Academy Trust

Email: info@wmat.org.uk

Address: Weydon Lane, Farnham, Surrey, GU9 8UG

IC Registration: ZA792813

Schools in this trust:

- Woolmer Hill School
- Weydon School
- Rodborough
- The Ridgeway School
- Eggar's School
- Crondall Primary School
- Farnham Heath End
- The Park School
- The Abbey School
- Frogmore Community College
- Brooklands School
- Beacon Hill Primary School
- Clifton Hill School
- Frimley Church of England School
- Tomlinscote School
- The Sixth Form College Farnborough
- St Mark's Church of England Primary School

> **NOTE**
> This policy covers any school that joins during the policy period and remains covered for its duration.

Data Protection Officer (DPO): Satswana Ltd

Email: GDPR@weydonmat.co.uk

Address: Suite G12 Ferneberga House, Alexandra Road, Farnborough, GU14 6DQ

IC Registration: ZB209055

Local Authority (LA):

- Surrey County Council
- Hampshire County Council

Readability: Grade 15 (Post-16 (ages 16+))

> **NOTE**
> Version control: The Key details are correct at the time of acceptance. If we need to make changes, we will update them at the next review date, 22/04/2027.

Policy statement

This notice explains:

- What personal data we hold about job applicants
- How we collect it
- How we use it
- Who we share it with

We must provide this information by law.

Who this notice applies to

This notice is for job applicants who apply:

- Directly to us, or
- Through a job site or agency

Definitions

Organisational and governance roles

Organisation references

Controller (Weydon Multi Academy Trust) is the organisation shown in the Key details section (including any subsidiary colleges or schools, organisations, and clubs).

College means a sixth form college, further education college, or other post-16 provider operated by, linked to, or working with Weydon Multi Academy Trust, where applicable.

We, us, our refers to Weydon Multi Academy Trust.

Governance / accountability

Senior Responsible Person (SRP) is the most senior individual within the setting. The SRP oversees day-to-day data protection management. The SRP may assign tasks to the Data Protection Officer or a Delegated Lead, and may delegate operational responsibilities.

Responsible Chair is the Chair of Trustees.

Trustee or Governor is an individual appointed either to the board of trustees of an academy trust (Trustee) or to a local governing body or a college or school level governance structure (Governor). Trustees hold ultimate accountability for the trust. Governors may have delegated responsibilities at local level. Trustees also act as charity trustees and company directors.

Weydon Multi Academy Trust's Data Protection Officer (DPO) is Satswana Ltd. Contact details are in the Key details section.

Delegated Lead (for the DPO) is an individual appointed in writing by the SRP to work with the DPO. They carry out defined data protection tasks (for example, breach triage, DPIA support, supplier checks, and training checks) within an agreed scope and escalation route.

Operational roles

Chief Operating Officer (COO) or Business Manager oversees the day-to-day running of the trust or school.

IT Representative manages and maintains the college or school's IT systems and provides technical support.

Social Media Representative is the individual responsible for managing the college or school's social media presence and supporting compliance.

Safeguarding and statutory partners

Designated Safeguarding Lead (DSL) is the senior member of staff responsible for safeguarding and child protection matters. This includes managing referrals, liaising with external agencies, and ensuring appropriate staff training.

Local Authority (LA) is the local government body responsible for education and children's services in its area. This includes admissions, attendance, SEND support, safeguarding, and public health functions. We may work with the LA to meet legal duties and manage incidents. Contact details are in the Key details section.

Department for Education (DFE) is the government department responsible for education.

Disclosure and Barring Service (DBS) is the UK body that supports safer recruitment by issuing criminal record information and, where eligible, barred list status. A DBS check may be basic, standard, or enhanced, and may include children's and/or adults' barred list information where legally permitted.

People and groups

Pupil (or student, learner, or young person) means a child or young person enrolled with us, including sixth form learners (16–19).

Parents means a parent, guardian, or carer with parental responsibility for a pupil at Weydon Multi Academy Trust.

Workforce means all staff and individuals working for or on behalf of Weydon Multi Academy Trust. This includes employees, agency staff, temporary staff, peripatetic staff, apprentices, trainees, and self-employed people providing services.

Volunteer is an individual who supports us without payment. Volunteers may help with reading, trips, classroom support, events, or specialist input.

Core GDPR roles

Data subject is any identifiable person whose personal data we hold or use.

Data controller is the person or organisation that decides why and how personal data is used.

Data processor is the person or organisation that processes personal data on behalf of the controller.

Legal rules and structure

The UK General Data Protection Regulation (UK GDPR) is the UK's version of GDPR, which has been retained in UK law. It sets out the main data protection rules, rights and duties, and is supported by the DPA 2018. The **EU General Data Protection Regulation (EU GDPR)** applies within the European Union.

The Data Protection Act 2018 (DPA 2018) is the UK's main data protection law. It works alongside UK GDPR and sets out UK-specific rules, exceptions, and enforcement.

The Data (Use and Access) Act 2025 (DUAA) changes data protection, digital checking, and smart data systems. Key education changes include the ability to pause subject access request time limits during school holidays ('stop the clock'). The Act also includes a legal fair and reasonable test for following information rules.

Information Commissioner (IC) is the UK's independent regulator for data protection, freedom of information and related rights. It ensures we comply with the Data Protection Act, the Freedom of Information Act, and UK GDPR, and handles official complaints. (Formerly known as the Information Commissioner's Office (ICO); renamed under the Data (Use and Access) Act 2025.)

The Freedom of Information Act 2000 (FOIA) gives a general right of access to recorded information held by public bodies, subject to legal exceptions.

Education (Pupil Information) (England) Regulations 2005 set out parents' rights to access their child's educational records and schools' duties to disclose them.

Education Act (EA) sets the legal rules for how education is organised, run, and provided in England, including school management, curriculum, attendance, and funding.

Keeping Children Safe in Education (KCSIE) is legal guidance for schools and colleges in England on safeguarding and safer hiring, issued by the Department for Education (DFE).

The Children Act 1989 is the main law in England and Wales setting out duties to safeguard and promote the welfare of children. It provides the legal framework for child protection, including local authority duties to investigate where a child may be at risk of significant harm.

Special educational needs and disability (SEND) Code of Practice is statutory guidance for England on duties towards children and young people with SEND (under the Children and Families Act 2014). Schools, colleges and local authorities must have regard to it.

The Equality Act 2010 is the UK's main anti-discrimination law. It protects people from unlawful discrimination, harassment and victimisation based on protected characteristics (including disability), and places a duty on public bodies (including schools and academy

trusts) to have due regard to eliminating discrimination, advancing equality of opportunity, and fostering good relations (the Public Sector Equality Duty).

Human Rights Act 1998 incorporates the European Convention on Human Rights into UK law, including the right to privacy.

The Protection of Freedoms Act 2012 (PoFA 2012) controls, among other things, the use of fingerprint and face data and surveillance, including rules on consent and management.

Computer Misuse Act 1990 criminalises unauthorised access to computer systems and data.

Data protection concepts

Data protection terms

Personal data means any information relating to an identified or identifiable living person (UK GDPR, Article 4(1)).

Processing means doing anything to personal data, such as collecting, recording, organising, structuring, storing, changing, using, sharing, erasing, or destroying it. Processing can be automated or manual.

Using special category and criminal offence data

We only use special category data and criminal offence data when we have a lawful basis (Article 6) and we meet the extra legal conditions that apply.

Special category data (Article 9)

We meet a relevant Article 9 condition. Common examples include:

- **Employment law:** processing is necessary to perform or exercise employment, social security, or social protection obligations or rights.
- **Vital interests:** the person cannot give consent (physically or legally unable), and we must protect their life or someone else's life.
- **Made public:** the person has already made the data public.
- **Legal claims:** we need the data to establish, exercise, or defend legal claims.
- **Public interest:** processing is required for substantial public interest as defined in law.
- **Health or social care:** a health or social care professional (or someone bound by confidentiality) needs the data to provide care.
- **Public health:** a health professional (or someone bound by confidentiality) needs the data for public health purposes.
- **Research or statistics:** processing is necessary for archiving, scientific or historical research, or statistics, and is in the public interest.

Criminal offence data (UK GDPR Article 10 and DPA 2018)

We meet an appropriate condition under UK law (Schedule 1, DPA 2018), where required.

Common examples include:

- **Vital interests:** the person cannot give consent (physically or legally unable), and we must protect their life or someone else's life.
- **Made public:** the person has already made the data public.
- **Legal proceedings:** we need the data for legal proceedings, to obtain legal advice, or to establish, exercise, or defend legal rights.
- **Public interest:** processing is required for substantial public interest as defined in law.

Personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data Protection Impact Assessment (DPIA) is a documented assessment used to identify and reduce data protection risks, particularly for high-risk processing or when introducing new technologies.

Lawful basis

Lawful basis means the legal reason we rely on to use personal data. Under the UK GDPR, we must have at least one lawful basis for each type of processing.

- **Consent** — Article 6(1)(a): the person has given a clear, informed choice for a specific purpose. Consent can be withdrawn.
- **Contract** — Article 6(1)(b): processing is necessary to perform a contract with the person, or to take steps at their request before entering a contract.
- **Legal obligation** — Article 6(1)(c): processing is necessary to comply with a legal duty that applies to us.
- **Vital interests** — Article 6(1)(d): processing is necessary to protect someone's life.
- **Public task (official authority)** — Article 6(1)(e): processing is necessary to perform a task in the public interest or in the exercise of official authority.
- **Legitimate interests** — Article 6(1)(f): processing is necessary for our (or someone else's) legitimate interests, as long as those interests are not overridden by the person's rights and freedoms.

Rights / requests

- **Data protection rights requests**
  - **Subject Access Request (SAR)** is when a person (or someone they authorise) asks to access their personal data and learn how it is used, under Articles 12–15 of the UK GDPR and the DPA 2018. We check identity and respond within statutory time limits. We may redact third-party data and apply exemptions where permitted.
  - **Other UK GDPR rights** (depending on the circumstances) include Rectification, Erasure, Restriction, Objection, and Data portability.
- **Freedom of information requests**
  - **Freedom of Information request (FOI)** is a request for recorded information made under the Freedom of Information Act 2000. It applies to public authorities and is separate from data protection rights, although requests may sometimes overlap.

Education-specific definitions

Parental responsibility means the rights, duties, powers, and authority that a parent (or another person) has for a child. Documents that may show parental responsibility include:

- Birth certificate
- Parental responsibility agreement
- Child arrangements order
- Step-parent parental responsibility agreement
- Guardianship order
- Parental responsibility order

Safeguarding means steps to protect the health, wellbeing, and rights of children and people who may need extra support, including preventing harm and abuse.

Records management

Retention schedule means the rules that set out how long records are kept and how they are securely disposed of.

Data minimisation techniques

Pseudonymisation replaces identifying information with an artificial identifier. It can be reversed if the additional information is kept separately and securely.

Anonymisation removes the ability to identify an individual, and cannot be reversed.

Technology terms

Artificial Intelligence (AI) means software or online services that use statistical or machine learning methods to generate outputs, make predictions, or support decisions. Outputs can include text, images, summaries, recommendations, classifications, or other content.

Generative AI means AI that creates new content in response to prompts (for example, text, images, audio, or code).

Automated decision-making means a decision made by a system without meaningful human involvement. Where this is used, we apply appropriate safeguards and human oversight.

Data protection principles

We follow data protection law.

This means we:

- Use data lawfully and fairly
- Tell you what we do with it
- Collect only what we need
- Keep it up to date

- Keep it only as long as needed
- Keep it secure

What data we may process

We collect data to run recruiting safely and fairly.

> **NOTE**
> We only do checks that apply to the role and that the law allows.

During recruiting, we may process:

- Name and contact details
- Recruitment details
  - Application form
  - CV
  - Supporting statement
  - Interview notes
- Key identifiers where needed
  - Date of birth
  - National Insurance number

Checks (often after a conditional offer) may include:

- ID and right-to-work checks
- References
- Qualification checks
- DBS checks (where required)
- Occupational health information
  - To support adjustments
  - To check fitness for the role

How we use your personal data

We use your personal data to:

- Assess suitability for the role
- Contact you about your application
- Carry out safer recruitment and safeguarding checks
- Meet equality and employment duties
- Keep our systems and premises secure

Where we get your data

Most of the data comes from you.

We may also get data from:

- Recruitment platforms or agencies
- Referees and previous employers
- Professional bodies
- Government bodies
  - Right-to-work checks
  - Disqualification checks

Filtering and monitoring

If you visit our site or use our systems during an interview or assessment, we may monitor use for safety and security.

This may include:

- Protecting devices and networks
- Looking into misuse
- Meeting legal duties

Who we share your personal data with

We share your data only when needed for recruiting, and only where the law allows.

This may include:

- Recruitment and HR providers
- Referees and previous employers
- Occupational health providers
- DBS bodies (where required)
- Our regulator (for example, Ofsted)
- Government departments or agencies
- Advisers (for example, legal or audit support)

How long we keep your data

We keep recruiting data only for as long as we need it, or for as long as the law requires.

As a general guide:

- **Unsuccessful applicants:** usually 6 months after the recruitment decision

> **NOTE**
> We may keep it longer if we need it to deal with a complaint or challenge.

- **Successful applicants:** moved into the staff record and kept under staff retention rules

Our legal bases for processing

We use personal data only when the law allows.

This is called a **lawful basis**.

We may rely on contract, legal duty, public task, or legitimate interests.

> **NOTE**
> Definitions are in the Definitions section.

Transparency and fairness

When we collect personal data from you, we will give you the details required by data protection law.

We also check fairness.

We will not use personal data in ways you would not expect.

We will not use it in ways that unfairly harm you.

Your rights

You can ask us to:

- Provide access to your personal data
- Correct inaccurate data
- Delete your data (where we are not required to keep it)
- Restrict or object to certain uses of your data

Some rights are not absolute.

We may need to keep or use data where the law requires it.

Contact our DPO if you want to use your rights.

Contact us

> **INFO**
> Contact us about data protection? Our college or school office can answer general questions or direct you to the right person. Contact: | info@wmat.org.uk

Identity verification: We may need to verify who you are before responding.

Help us respond faster: Tell us which school you are asking about.

Complaints about data protection

This section is only for complaints about how we handle your personal data.

> **NOTE**
> For general college or school complaints (behaviour, teaching, admissions, etc.), please follow the college or school's Complaints Policy.

Data protection concerns? Contact our DPO (see Key details above) if you have concerns about how we collect, use, or share your personal information.

Formal data protection complaint? If you want to make a formal complaint about our data protection practices, contact our DPO in writing GDPR@weydonmat.co.uk. We will investigate and respond within one month.

Still not satisfied? You can complain to the Information Commissioner:

Address: Information Commissioner's Office Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF **Telephone:** 0303 123 1113 **Online:** https://ico.org.uk/make-a-complaint/