Data Protection Policy

Policy Last Review: January 2026
This policy will be reviewed every 12 months
Review Date: January 2027

Compliance Lead: Mihai Manole
Compliance Lead Contact Details: compliance@winnereducation.co.uk | 0121 353 1661

1. About This Policy

1.1 Winner Education Ltd ("the Company") processes personal data relating to employees, workers (including agency workers), candidates, and contractors. We are committed to handling personal data lawfully, fairly, and transparently in accordance with the UK GDPR and the Data Protection Act 2018.

1.2 This policy explains how we collect, use, store, and protect personal data during recruitment, engagement, and throughout the working relationship.

1.3 This policy applies to:

- Employees (permanent and fixed term)
- Agency workers and temporary workers supplied to clients
- Candidates and prospective workers

1.4 This policy does not form part of any contract of employment or engagement and may be updated at any time.

2. Data Protection Principles

We comply with the UK GDPR principles. Personal data must be:

(a) Processed lawfully, fairly, and transparently
(b) Collected for specified, explicit, and legitimate purposes
(c) Adequate, relevant, and limited to what is necessary
(d) Accurate and kept up to date
(e) Kept only for as long as necessary
(f) Processed securely (integrity and confidentiality)
(g) Accountable – we must demonstrate compliance

3. Definitions

- **Personal Data**: Any information that identifies or could identify an individual (e.g. name, address, NI number, CV, DBS information).
- **Special Category Data**: Sensitive data such as health, ethnicity, religion, criminal records (relevant for safer recruitment).
- **Processing**: Any operation performed on personal data (e.g. collection, storage, use, sharing, deletion).

4. Lawful Basis for Processing

4.1 We process personal data under one or more lawful bases:

- Contractual necessity (e.g. pay, placement)
- Legal obligation (e.g. Right to Work checks, safeguarding)
- Legitimate interests (e.g. recruitment, business operations)

- Consent (where required, e.g. marketing)

4.2 For special category data, we rely on:

- Employment and social security obligations
- Safeguarding requirements (particularly in education settings)
- Explicit consent (where appropriate)

5. Safer Recruitment & Compliance (APSCo Alignment)

5.1 In line with APSCo and safeguarding requirements, we process personal data to:

- Verify identity and Right to Work in the UK
- Conduct DBS checks (where required)
- Obtain references and employment history
- Assess suitability to work with children or vulnerable individuals
- Maintain compliance records for audit purposes

5.2 We ensure:

- Data collected is strictly necessary for safeguarding and compliance
- Information is handled confidentially and securely
- Only authorised personnel access sensitive data

6. How We Use Personal Data

We use personal data for:

6.1 Recruitment & Onboarding

- Assessing suitability for roles
- Conducting interviews and compliance checks
- Maintaining candidate records

6.2 Employment / Engagement Management

- Payroll, tax, and pension administration
- Absence and performance management
- Training and development
- Health and safety monitoring

6.3 Placement & Client Services

- Supplying workers to clients
- Managing assignments and timesheets
- Communicating with clients regarding staffing

6.4 Legal & Regulatory Compliance

- Safeguarding obligations in education
- Immigration and Right to Work compliance
- Responding to regulators (e.g. HMRC, Home Office)

7. Data Minimisation

We only collect and process personal data that is necessary for legitimate business and legal purposes. Excess or irrelevant data will not be retained.

8. Accuracy of Data

8.1 We take reasonable steps to ensure data is accurate and up to date.
8.2 Individuals must inform us of any changes (e.g. address, right to work status).
8.3 Inaccurate data will be corrected or deleted promptly.

9. Data Retention

9.1 Personal data is retained only as long as necessary and in line with legal and APSCo guidance.

Typical retention periods include:

- Candidate data (unsuccessful): up to 12 months
- Worker/employee records: 6 years after engagement ends
- Safeguarding/DBS records: in line with statutory guidance
- Payroll/tax records: 6 years (HMRC requirement)

9.2 Secure deletion or anonymisation will be applied once data is no longer required.

10. Individual Rights

Individuals have the right to:

- Access their personal data (Subject Access Request)
- Request correction of inaccurate data
- Request erasure (where applicable)
- Restrict or object to processing
- Data portability (where applicable)
- Not be subject to solely automated decision-making

Requests should be submitted in writing to HR or the Compliance Lead.

11. Data Security

11.1 We implement appropriate technical and organisational measures, including:

- Secure IT systems and access controls
- Password protection and encryption
- Staff training on data protection
- Secure storage (physical and electronic)

11.2 Access to personal data is restricted to authorised personnel only.

12. Sharing Data with Third Parties

12.1 We may share personal data with:

- Clients (for placement purposes)
- Payroll providers and pension schemes
- Compliance bodies (e.g. DBS, Home Office)
- Regulators and legal authorities

12.2 We ensure:

- Data sharing is lawful and necessary
- Data processing agreements are in place where required
- Third parties maintain appropriate security standards

13. International Transfers

We do not transfer personal data outside the UK unless adequate safeguards are in place in accordance with UK GDPR.

14. Data Breaches

14.1 Any suspected data breach must be reported immediately to HR or the Data Protection Lead.

14.2 We will:

- Investigate and contain the breach
- Notify the ICO where required
- Inform affected individuals where there is a risk to their rights

15. Subject Access Requests (SARs)

Requests must be made in writing to HR.
We will respond within one month in accordance with UK GDPR.

16. Responsibilities

- **All staff and workers**: must comply with this policy and handle data responsibly
- **Managers**: ensure compliance within their teams

- **HR / Compliance**: oversee implementation and monitoring

17. Breach of Policy

Failure to comply with this policy may result in:

- Disciplinary action (employees)
- Termination of assignment or contract (agency workers)
- Legal action where appropriate

18. Review

This policy will be reviewed annually or in line with legislative or APSCo guidance changes.