WC14 – Data Protection Policy

Westerfield College | College Policy

Field	Details
Document Reference	WC14
Document Title	Data Protection Policy
Status	Published
Version	Version 1
Last Updated	18 December 2025
Policy Owner	Data Protection Officer (DPO)
Approved By	Board
Next Review Date	December 2026

1. Purpose

This Data Protection Policy ensures Westerfield College:

- Complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and follows good practice
- Protects the data privacy and protection rights of staff, students, business partners, and all other stakeholders
- Is transparent about how it processes individuals' personal data
- Protects itself from the risks of a data breach and associated regulatory penalties
- Facilitates the rights of individuals under the UK GDPR (Articles 15–21)
- Ensures ongoing adherence and continuous improvement in data privacy and protection practices

2. Scope

This policy applies to:

- All personal data processed by Westerfield College, regardless of the medium in which it is held (digital or paper-based)
- All staff (full-time, part-time, and temporary), volunteers, contractors, and third parties who process personal data on behalf of the College
- All systems, processes, and activities that involve the collection, storage, use, sharing, or disposal of personal data

Non-compliance with this policy may result in disciplinary action, up to and including dismissal, and may expose the College to regulatory investigation and financial penalties under the UK GDPR.

3. Data Protection Principles

Westerfield College is committed to processing personal data in accordance with its responsibilities under the UK GDPR. Article 5 requires that personal data shall be:

- Processed lawfully, fairly, and in a transparent manner in relation to individuals (Lawfulness, Fairness, Transparency)
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose Limitation)
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation)
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure inaccurate personal data is erased or rectified without delay (Accuracy)
- Kept in a form that permits identification of data subjects for no longer than is necessary (Storage Limitation)
- Processed in a manner that ensures appropriate security against unauthorised or unlawful processing and accidental loss, destruction, or damage (Integrity and Confidentiality)

4. General Provisions

- This policy applies to all personal data processed by Westerfield College under the UK GDPR
- The Data Protection Officer (DPO) is responsible for the College's ongoing compliance with this policy and reports directly to the Westerfield Management Team. The DPO can be contacted at: dpo@westerfieldcollege.uk
- Westerfield College is registered with the Information Commissioner's Office (ICO) as an organisation that processes personal data and will maintain that registration at all times

5. Data Transparency and Openness

- At the point of collection, all individuals shall be directed to the College's Privacy Notice, providing a clear explanation of how their data will be processed, the lawful basis, with whom it may be shared, and how they may exercise their rights
- The College shall maintain a publicly accessible, up-to-date Privacy Notice on its website
- All Data Subject Access Requests (DSARs) shall be acknowledged within 5 working days and responded to within one calendar month
- The College shall maintain an appropriate set of policies, procedures, and training materials, reviewed at least annually

6. Lawful Purposes

- All data processed by Westerfield College must rely on one of the six lawful bases under Article 6 of the UK GDPR: consent, contract, legal obligation, vital interests, public task, or legitimate interests
- The College shall record the appropriate lawful basis in the Lawful Basis for Processing Personal Data register
- Where consent is relied upon, evidence of opt-in consent shall be recorded and maintained. Individuals must be able to withdraw consent at any time and such withdrawal shall be promptly reflected in the College's systems
- Where Legitimate Interest is relied upon, a Legitimate Interest Assessment (LIA) shall be completed and documented before processing commences

7. Data Minimisation

- Westerfield College shall ensure that personal data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed
- Special Category Data (Article 9, UK GDPR) — including racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, and data concerning sex life or sexual orientation — shall only be collected with the prior written permission of the DPO and only where a valid Article 9 condition exists

8. Data Accuracy

- Westerfield College shall take reasonable steps to ensure that all personal data held is accurate
- Where necessary, the College shall establish processes to keep personal data up to date
- Individuals are encouraged to notify the College of any changes to their personal data, and the College shall provide simple mechanisms to enable them to do so

9. Storage Limitation

- Westerfield College shall maintain a Records Management, Retention, and Disposal Policy to guide staff on handling records and to define retention and disposal requirements
- The College shall maintain a Data Retention Schedule for each category of personal data processed, specifying retention periods and the lawful basis for retention
- The Data Retention Schedule shall take account of relevant national legislation in addition to the requirements of the UK GDPR
- As a general principle, personal data relating to individuals (including students and staff) shall be retained for a period of two (2) years from the date of last activity or the end of the individual's relationship with the College, unless a longer period is required by law or legitimate business need
- Personal data that has reached the end of its retention period shall be disposed of securely and in a manner that renders it irrecoverable

10. Data Confidentiality and Security

- Westerfield College shall maintain an Information Security Policy describing how it protects personal data and other sensitive information
- All personal data shall be stored using modern, up-to-date software with appropriate encryption where required
- Access to personal data shall be role-based, limited to staff who require access to fulfil their duties, with appropriate authentication controls maintained
- When personal data is deleted, it shall be done securely such that the data is rendered irrecoverable
- Appropriate backup and disaster recovery solutions shall be in place, tested regularly, with records of testing maintained
- Where personal data is shared internally or with external organisations, its security shall be governed by appropriate Data Sharing Agreements and Data Processing Agreements (DPAs)

11. International Data Transfers

- Westerfield College shall not transfer personal data outside the UK unless that country ensures an adequate level of protection, or appropriate safeguards (such as Standard Contractual Clauses) are in place
- Any proposed international data transfer must be approved by the DPO prior to commencement
- A record of all international data transfers shall be maintained within the College's Records of Processing Activities (ROPA)

12. Data Processors and Third Parties

- Where Westerfield College engages third parties to process personal data on its behalf, a written Data Processing Agreement (DPA) shall be in place before any data is shared
- Third-party processors shall be subject to due diligence assessment prior to engagement and shall provide sufficient guarantees as to their technical and organisational security measures
- The College shall maintain an up-to-date register of all data processors

13. Data Breach Management

- In the event of a personal data breach, Westerfield College shall promptly assess the risk to individuals' rights and freedoms
- Where the breach is likely to result in a risk to individuals, the College shall notify the ICO without undue delay and within 72 hours of becoming aware (Article 33, UK GDPR)
- Where the breach is likely to result in a high risk to individuals, the College shall also notify the affected individuals without undue delay (Article 34, UK GDPR)

- The College shall maintain a Data Breach Procedure and a Data Breach Register, recording all breaches regardless of whether ICO notification was required
- All staff shall report suspected data breaches to the DPO immediately upon becoming aware of them

14. Individual Rights

Westerfield College shall maintain suitable procedures to facilitate individuals' data rights as defined in the UK GDPR (Articles 13–21):

Right	Summary
Right to be Informed (Arts. 13–14)	Individuals must be told how their data is used at point of collection
Right of Access (Art. 15)	Individuals can request a copy of their personal data (DSAR)
Right to Rectification (Art. 16)	Individuals can request correction of inaccurate data
Right to Erasure (Art. 17)	Individuals can request deletion of their data in certain circumstances
Right to Restriction (Art. 18)	Individuals can request that processing of their data is restricted
Right to Data Portability (Art. 20)	Individuals can request their data in a machine-readable format
Right to Object (Art. 21)	Individuals can object to processing based on legitimate interest or direct marketing
Rights re. Automated Decisions (Art. 22)	Individuals have rights not to be subject to solely automated decisions that significantly affect them

- The College shall maintain a simple, accessible DSAR guide and process to allow timely and compliant responses
- Requests shall be responded to within one calendar month; this may be extended by a further two months for complex or multiple requests, with the requester notified accordingly

15. Compliance and Training

- Westerfield College shall maintain a Data Protection organisational structure that enables effective discharge of its data privacy obligations
- A Privacy by Design approach shall be embedded into all business processes, projects, and systems involving the processing of personal data
- All staff shall have access to a Data Protection Handbook providing clear, practical guidance on GDPR-compliant working practices
- All new staff shall complete GDPR awareness training as part of their induction; all staff shall undertake refresher training at least every two years
- Training records shall be maintained and reported to the Management Team

- An audit schedule shall be maintained ensuring all sites and shared-services functions are audited at least annually
- An annual organisational GDPR audit shall be conducted and its results reported to the Academic Board
- The College shall conduct regular Information Security testing and remediate identified vulnerabilities

16. Continuous Improvement

- Westerfield College shall seek regular feedback from individuals and staff on how data protection practices could be improved
- Audits shall be conducted in an educational and supportive manner, with findings used to share best practice across the organisation
- The College shall subscribe to and participate in appropriate professional organisations, forums, and news sources to monitor global developments and disseminate best practice internally

Policy Review

This policy will be reviewed every two years by the Academic Board, or earlier if required by internal changes or legislative amendments. The DPO is responsible for initiating the review and presenting recommendations to the Board.

Version History

No.	Revised On	Version	Changes	Approved By	Date	Revised By
1	18 Dec 202	1.0	Initial publication	Academic Board	Dec 2026	DPO