



GREEN VALLEY ACADEMY

IT, Data Protection and Data Security Policy

Approved: October 2026

DOCUMENT CONTROL

Reference	GVA-25 (supersedes and expands the earlier Data Protection framework section)
Policy owner	Data Protection Lead — Academic Registrar and Admissions Officer; infrastructure security operated with group IT support
Approved by	Academic Board— 5 October 2026
Effective from	5 October 2026
Next review	October 2027, and after any significant incident
Applies to	All staff, students and contractors; all personal data in any format; all Academy systems, devices and approved services
Linked documents	Data Breach Reporting Form (Form 7); Subject Access Request Form (Form 5); Compliance Policy; University of Wolverhampton data-sharing provisions; Safeguarding and Prevent Policy

CONTENTS

DOCUMENT CONTROL

1. PURPOSE AND SCOPE
2. PRINCIPLES AND ACCOUNTABILITY
3. ROLES AND RESPONSIBILITIES
4. LAWFUL, FAIR AND TRANSPARENT PROCESSING
5. DATA SECURITY
6. INDIVIDUALS' RIGHTS
7. PERSONAL DATA BREACH RESPONSE
8. ACCEPTABLE USE, TRAINING AND MONITORING
9. RETENTION AND DISPOSAL

APPENDIX A — RETENTION SCHEDULE (SUMMARY)

If page numbers do not display, right-click the contents and select "Update Field".

1. PURPOSE AND SCOPE

- 1.1** This policy governs how Green Valley Academy collects, uses, stores, secures, shares, retains and disposes of personal data, and how it protects the information technology upon which that data depends. It applies to the personal data of applicants, students, staff, members of the Board, contractors and visitors; to every format in which data is held, digital and paper alike; and to every system used in the Academy's business, including the student record system, the virtual learning environment, email and telephony, CCTV, and every approved cloud service. The Academy is registered with the Information Commissioner's Office as a data controller ICO registration number ZA77153, renewal date 11 July 2027; this policy is the principal instrument through which the Academy discharges its obligations under the UK General Data Protection Regulation and the Data Protection Act 2018.

2. PRINCIPLES AND ACCOUNTABILITY

- 2.1** All processing of personal data by or for the Academy shall observe the statutory principles: it shall be lawful, fair and transparent; collected for specified, explicit and legitimate purposes and not further processed incompatibly; adequate, relevant and limited to what is necessary; accurate and kept up to date, with inaccuracies rectified without delay; kept in identifiable form no longer than necessary, in accordance with the retention schedule at Appendix A; and processed with appropriate security, integrity and confidentiality. In accordance with the accountability principle, the Academy shall maintain, and the Data Protection Lead shall keep current, the records which demonstrate compliance: a record of processing activities; the privacy notices issued to each category of data subject; records of consent where consent is the lawful basis; data-sharing documentation, including the provisions applying between the Academy and the University of Wolverhampton; data protection impact assessments; the breach register; and the training record.

3. ROLES AND RESPONSIBILITIES

- 3.1** The Data Protection Lead is the Academic Registrar and Admissions Officer, who is the first point of contact for all data protection matters; coordinates subject access and other rights requests; leads breach response under Section 7; advises on and records data protection impact assessments; maintains the accountability records in clause 2.2; and reports at least annually to the Board of Directors. The Principal is accountable for the resourcing of these arrangements and personally signs off every external data return under the internal control provisions of the Compliance Policy. Group IT support operates on the technical infrastructure — identity and access management, patching, endpoint protection, filtering, backup and monitoring — to the standards in Section 5. Every member of staff is responsible for handling personal data only as their role requires, for completing training at induction and annually, and for reporting any suspected breach immediately under Section 7; and every student is responsible for observing the acceptable-use expectations in Section 8.

4. LAWFUL, FAIR AND TRANSPARENT PROCESSING

- 4.1** The Academy shall identify and document a lawful basis for every processing purpose before processing begins and shall communicate it through privacy notices issued to applicants, students and staff at the point of collection, each notice stating what is collected, why, under what basis, with whom it is shared, how long it is kept, and the rights available. Special category data — including health, disability, safeguarding, and the demographic data collected for equality monitoring — shall be processed only where an additional condition is identified and documented, shall be accessible only to the named roles whose functions require it, and shall be stored separately where this policy or a linked policy so requires. Personal data shall be shared with the University of Wolverhampton only as required for registration, assessment, award and quality assurance under the franchise agreement's data-sharing provisions; with statutory bodies where the law requires; and otherwise only where a documented basis exists, no routine disclosure being made to any other party. Direct marketing shall be conducted only with consent or within the soft opt-in, always with a working unsubscribe, and the Academy shall neither purchase nor sell marketing lists. A data protection impact assessment shall be completed, and its mitigations implemented, before any new system or processing likely to result in high risk is introduced, including the student record system, the virtual learning environment, CCTV, and any analytics applied to student engagement data.

5. DATA SECURITY

- 5.1** The technical controls operated by or for the Academy shall include: role-based access on least-privilege principles, reviewed termly and revoked on the day a user leaves; multi-factor authentication on all staff accounts and administrative access; encryption of laptops, portable devices and removable media, with personal data prohibited on personal devices except through approved, containerised applications; supported and patched operating systems and applications, with endpoint protection and logging; email and web filtering, the latter configured also to serve the Prevent duty under the Safeguarding and Prevent Policy in a manner proportionate and transparent to users; daily backups, stored separately, with restoration tested at least termly; and certification to Cyber Essentials, maintained continuously. Target date: 01 November 2026
- 5.2** The organisational controls shall include: clear-desk and lock-screen practice; paper records containing personal data locked away when unattended and removed from campus only with the Data Protection Lead's approval; confidential waste shredded or destroyed by a certificated contractor; devices sanitised or destroyed before disposal, with a disposal log kept; suppliers who process personal data engaged only under written contracts containing the processor clauses required by Article 28, following documented due diligence and with international transfers permitted only under a lawful transfer mechanism; and no unsupervised access to records or systems by visitors or contractors.

6. INDIVIDUALS' RIGHTS

- 6.1** The Academy shall give effect to every right conferred by data protection law — access, rectification, erasure, restriction, portability, objection, and rights concerning automated decision-making — and shall treat the exercise of a right as a routine entitlement and never as a complaint or provocation. Requests may be made through the Subject Access Request Form (Form 5) or by any other route, and however received shall be logged by the Data Protection Lead on the day of receipt; identity shall be verified proportionately; the response shall be provided within one calendar month, extendable by up to two further months only for complex or numerous requests and with the requester informed of the extension and reasons within the first month; exemptions, third-party data and mixed records shall be handled in accordance with ICO guidance, with redactions recorded; and the outcome, and the requester's right to complain to the ICO, shall be stated in every response.

7. PERSONAL DATA BREACH RESPONSE

- 7.1** A personal data breach — any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data — shall be reported by any member of staff or student who becomes aware of it immediately, through Form 7 or directly to dataprotection@greenvalleyacademy.co.uk, and no person shall attempt to contain or investigate a breach alone before reporting it. Upon report, the Data Protection Lead shall follow the process at Figure 1: immediate containment; assessment of the data, individuals and risks involved; entry in the breach register, which records every breach whether or not notifiable; notification to the Information Commissioner's Office within seventy-two hours of awareness where the breach is likely to result in a risk to individuals' rights and freedoms, the clock running through weekends and holidays; communication without undue delay to affected individuals where the risk is high, in clear language and with practical advice; notification to the University of Wolverhampton where partnership data is affected, and to insurers where relevant; and a post-incident review addressing cause, controls and training, reported to the Executive Board and the Audit and Risk Committee. The honest reporting of a breach, including one the reporter caused, shall always be treated constructively; the concealment of a breach is gross misconduct.

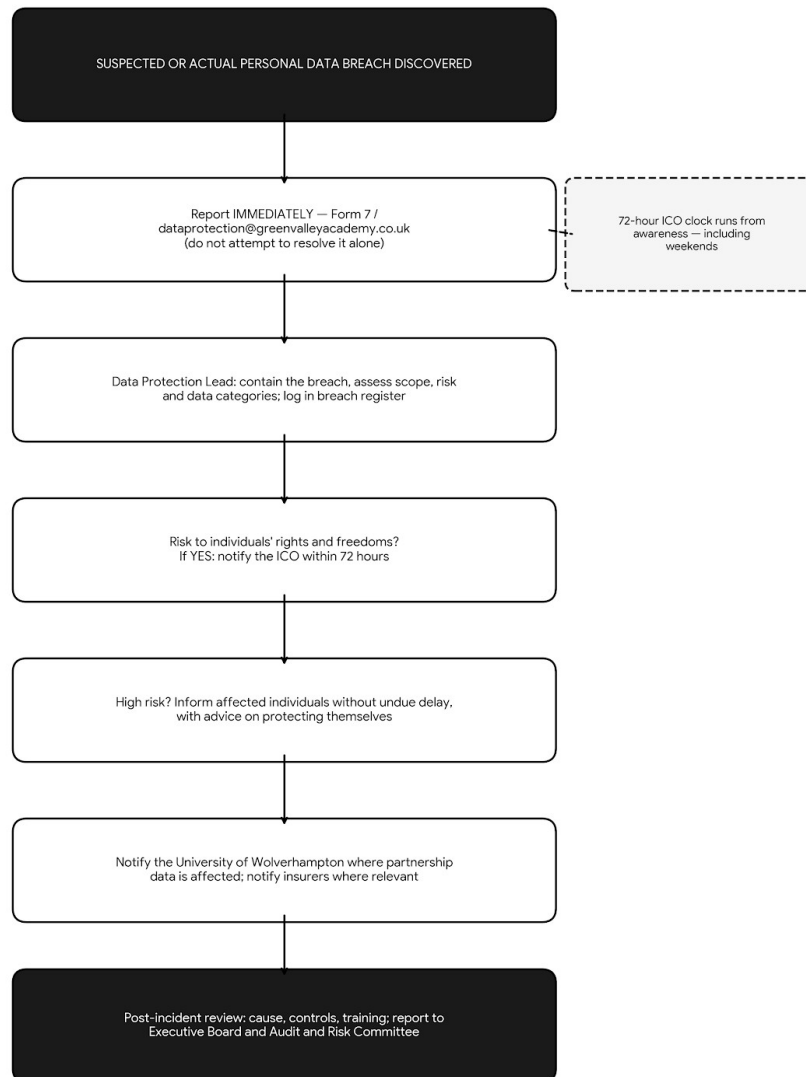


Figure 1: Personal data breach response process

8. ACCEPTABLE USE, TRAINING AND MONITORING

- 8.1** Staff and students shall use Academy systems in accordance with the acceptable-use expectations issued at induction, which include: use of Academy accounts and systems for Academy purposes; no sharing of credentials and no use of another person's account; no installation of unauthorised software and no circumvention of security controls; vigilance against phishing, with a one-click route for reporting suspicious messages; and respectful, lawful conduct in all electronic communication, to which the Academy's conduct policies apply as fully as they do in person. The Academy's monitoring of systems shall be proportionate, documented, and disclosed in the privacy notices. All staff shall complete data protection and security training at induction and annually, with completion recorded and reported termly to the Executive Board; and the Data Protection Lead shall report annually to the Board of Directors on requests, breaches, impact assessments, training and registration.

9. RETENTION AND DISPOSAL

- 9.1** Personal data shall be retained no longer than necessary for the purpose for which it is held, in accordance with the schedule at Appendix A; where a requirement of the University of Wolverhampton, of statute or of limitation periods prescribes a longer period, the longer period shall apply and shall be recorded against the record set concerned. Disposal at the end of retention shall be secure, and significant record sets shall be logged. This policy shall be reviewed annually and after any significant incident, and any material amendment shall be approved by the Board of Directors.

APPENDIX A — RETENTION SCHEDULE (SUMMARY)

Record set	Retention period	Basis
Applications — unsuccessful	One year after the end of the admissions cycle; equality data anonymised thereafter	Business need; equality monitoring
Student academic records	Six years after completion; award data as required by the University of Wolverhampton	Partnership requirements; limitation
Safeguarding records	Until the person's 25th birthday, or seven years after last contact, whichever is later, subject to current statutory guidance	Safeguarding guidance
Wellbeing and support case notes	Six years after case closure	Duty of care; limitation
Staff records	Six years after employment ends	Employment law; limitation
Financial records	Six years from the end of the financial year	Tax and audit
CCTV recordings	Thirty days, unless preserved for an identified incident	Security
Breach, SAR and rights-request logs	Six years	Accountability

- A.1** The full retention schedule, covering every record set the Academy holds, is maintained by the Data Protection Lead and adopted alongside this policy. The full retention schedule, covering every record set held by the Academy, is maintained by the Data Protection Lead and was adopted alongside this policy on 5 October 2026.