



GREEN VALLEY ACADEMY

Data Protection and Data Security Policy Statement

Approved: October 2026

DOCUMENT CONTROL

Reference	GVA-08
Policy owner	Data Protection Lead — Academic Registrar and Admissions Officer
Approved by	Board of Directors — August 2026
Effective from	5 October 2026
Next review	October 2027
Applies to	All personal data processed by GVA, in every format and system
Linked documents	IT, Data Protection and Data Security Policy (detailed instrument); Data Breach Reporting Form; Subject Access Request Form; University of Wolverhampton data-sharing provisions and Student Privacy Notice

CONTENTS

DOCUMENT CONTROL

- 1. POLICY STATEMENT**
- 2. INDIVIDUALS' RIGHTS AND HOW THEY ARE HONOURED**
- 3. SECURITY AND EVERYDAY DISCIPLINE**
- 4. OPERATION AND GOVERNANCE**

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

1. POLICY STATEMENT

- 1.1** GVA processes personal data in accordance with the UK General Data Protection Regulation and the Data Protection Act 2018, is registered with the Information Commissioner's Office as a data controller, and binds itself to the statutory principles: lawful, fair and transparent processing under published privacy notices; purpose limitation and data minimisation; accuracy; retention no longer than necessary under a published schedule; and security appropriate to the risk, including role-based access, multi-factor authentication, encryption and tested backups. Because GVA's students are registered students at the University of Wolverhampton, student data is shared with the University as required for registration, assessment, award and quality assurance under the franchise agreement's data-sharing provisions, and students are informed of that sharing through the privacy notices and the University's own Student Privacy Notice; no other routine disclosure occurs without a documented lawful basis. Every rights request is honored within statutory timescales; every suspected breach is reported internally at once and to the ICO within seventy-two hours where the risk threshold is met; and every dataset or return provided to the University or any external body is reconciled and signed off before submission, the knowing submission of false data being gross misconduct.

2. INDIVIDUALS' RIGHTS AND HOW THEY ARE HONOURED

- 2.1** Every student, applicant, member of staff and other data subject may exercise, free of charge and without giving reasons, the rights the legislation confers: access to their personal data through a subject access request, submitted on the Subject Access Request Form or in any written form, answered within one calendar month with the extensions the law permits for complex requests; rectification of inaccurate data without delay; erasure, restriction of processing and objection, honored wherever the legal conditions are met and explained plainly where an exemption applies — for example where GVA must retain records of assessment or registration for the University of Wolverhampton's award purposes; data portability where applicable; and the right to complain to the Information Commissioner's Office at any time, which GVA states in its privacy notices and in every rights-request response. Rights requests are logged centrally by the Data Protection Lead, identity is verified before disclosure, third-party data is redacted with care, and no person shall ever suffer detriment for exercising a data protection right.

3. SECURITY AND EVERYDAY DISCIPLINE

- 3.1** The everyday obligations of staff and students are few and absolute: access systems only with your own credentials, protected by multi-factor authentication, and never share them; store personal data only in GVA's approved systems, never in personal accounts, personal devices outside the approved mobile-device arrangements, or unapproved cloud services; send personal data outside GVA only through approved, secure channels, checking recipients before sending; lock screens, secure papers, and collect printing promptly; complete data protection training at induction and annually; and report any suspected breach — a misdirected email, a lost device, unexpected system behavior, a paper file left exposed — immediately to the Data Protection Lead through

the Data Breach Reporting Form, because the seventy-two-hour statutory clock runs from GVA's awareness and early reporting is the difference between containment and harm. Suppliers processing personal data on GVA's behalf are engaged only under written contracts meeting the legislation processor requirements, with due diligence recorded before engagement and access ended promptly at contract close.

4. OPERATION AND GOVERNANCE

- 4.1** The detailed instrument — roles, technical and organisational controls, rights procedures, breach response with flowchart, acceptable use, and the retention schedule — is GVA's IT, Data Protection and Data Security Policy, approved by the Board and binding on all staff and students; this statement records the commitments from which it may never depart. The Data Protection Lead reports annually to the Board of Directors on requests, breaches, impact assessments, training and registration; the Audit and Risk Committee reviews the breach register; and this statement is reviewed annually.