Oakswood College

Empowering Through Education

Data Protection

Policy and Procedure

PROMOTING EXCELLENCE • ENSURING COMPLIANCE
SUPPORTING OUR COMMUNITY

GOVERNANCE | QUALITY | COMPLIANCE | EXCELLENCE

Oakswood College
Empowering Through Education

Oakswood College
Empowering Through Education

(Trading name of Oakswood Group Ltd)

DATA PROTECTION POLICY AND PROCEDURE (PRIVACY STANDARD)

Document Control & Version History

Field	Details
Document Title	Data Protection Policy (Privacy Standard)
Document Type	Governance & Compliance Policy
Publication Type	Public
Policy Owner	Head of Governance, Quality, Compliance & Information Systems
Accountable Officer	Chief Executive Officer
Approved By	Board of Governors
Approval Date	25 March 2026
Effective From	25 March 2026
Applies To	All staff, governors, students, contractors, third-party processors, and any individuals whose personal data is processed by Oakswood College
Last Reviewed	25 March 2026
Next Review Date	25 March 2027
Review Cycle	Annual
Version	1.0

Oakswood College
Empowering Through Education

TABLE OF CONTENTS

1. POLICY STATEMENT

1.1. Individuals have legal rights over how their personal information is used. In the course of its activities, Oakswood College will collect, use and store personal information about staff, students, applicants, alumni, customers, partners, suppliers and other contacts, and recognises its responsibility to handle that information lawfully and appropriately.

1.2. The categories of personal information Oakswood College may process include details about current, former and prospective employees, students, customers, alumni and suppliers, and other individuals it interacts with. This information may be stored on paper, in electronic systems or in other formats and is protected by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and related UK data protection legislation, which set out how such information may be used.

1.3. Oakswood College is committed to processing personal data in line with these laws and expects all staff and others working on its behalf to comply with this policy and associated procedures. Where any third party handles personal data for Oakswood College, appropriate measures will be taken to ensure that they meet equivalent standards of data protection.

1.4. This Data Protection Policy (Privacy Standard) is a non-contractual document and may be updated or withdrawn at any time. Breaches of this policy may be treated as a disciplinary matter.

2. DATA PROTECTION PRINCIPLES

2.1. Anyone who handles personal data on behalf of Oakswood College must comply with the following data protection principles. Personal data must be:

(a) Processed lawfully, fairly and in a transparent manner.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (purpose limitation).

(c) Adequate, relevant and limited to what is necessary for the purposes for which it is processed (data minimisation).

(d) Accurate and, where necessary, kept up to date (accuracy).

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed (storage limitation).

(f) Processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using suitable technical or organisational measures (security, integrity and confidentiality).

(g) Not transferred outside the UK/EEA unless appropriate safeguards are in place (transfer limitation).

(h) Processed in a way that upholds the rights of data subjects (data subject rights and requests).

2.2. Oakswood College is accountable for compliance with these principles and must be able to demonstrate that it meets them.

3. STATUS AND SCOPE OF THE POLICY

3.1. This policy sets out Oakswood College's approach to data protection and the conditions which must be satisfied when personal data is collected, used, stored, shared, transported and destroyed.

3.2. The policy applies to all staff and workers (including employees, agency workers, contractors, consultants, volunteers and interns) and to any other individuals who have access to personal data on behalf of Oakswood College, regardless of location or medium.

3.3. A designated person is responsible for overseeing compliance with this policy and applicable data protection law, and for providing advice and guidance. Staff should raise any questions or concerns about data protection with their line manager or the Head of GQC & IS (Head of Governance, Quality, Compliance & Information Systems) in the first instance.

3.4. Anyone who believes that this policy has not been followed in relation to their own personal data, or the personal data of someone else, should report their concerns to their manager or the Head of GQC & IS without delay.

4. KEY DEFINITIONS

4.1. **Personal Data** (referred to as "Data" in this policy) is any information relating to an identified or identifiable living individual. An individual can be identified directly or indirectly, for example through a name, identification number, location data, online identifier or factors specific to physical, physiological, genetic, mental, economic, cultural or social identity. Personal data can include factual information (such as contact details) or opinions (such as performance comments).

4.2. **Data Subjects** are the living individuals whose personal data is processed by Oakswood College. They may be, for example, staff, students, applicants, alumni, visiting artists, service users, customers, suppliers or other contacts. A data subject does not have to be a UK national or resident.

4.3. A **Data Controller** is the organisation or person that determines the purposes and means of processing personal data. Oakswood College acts as Data Controller for the personal data it uses in connection with its activities.

4.4. **Data Users** are members of staff or others working for Oakswood College whose roles involve accessing or handling personal data. Data Users must protect the data they work with and follow this policy and all related information security procedures.

4.5. **Data Processors** are organisations or individuals (other than Institution staff) who process personal data on behalf of Oakswood College, for example providers of IT systems, cloud services, mailing services or outsourced functions.

4.6. **Processing** is any activity involving personal data, whether automated or not. It includes obtaining, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, transmitting, disseminating, combining, restricting, erasing or destroying personal data, as well as making it available to others.

4.7**. Special Category Data** is a subset of personal data that is more sensitive and therefore needs higher protection. It includes data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data and data concerning a person's sex life or sexual orientation.

4.8. **Criminal Offence Data** is personal data relating to criminal convictions and offences, or related security measures.

4.9. **A Personal Data Breach** is any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, or any compromise of the security, confidentiality, integrity or availability of that data or its protective measures.

5. FAIR AND LAWFUL PROCESSING

5.1. Data protection law does not prevent Oakswood College from using personal data, but requires that it does so fairly, lawfully and in a way that respects individuals.

5.2. Personal data may only be processed where at least one lawful basis applies. **The main lawful bases** relied upon by Oakswood College are:

- **performance of a contract** (for example an employment contract or student contract)
- **compliance with a legal obligation**
- **legitimate interests** pursued by Oakswood College or a third party, provided these are not overridden by the data subject's interests or fundamental rights
- protection of someone's **vital interests**

- **performance of a task carried out in the public interest**
- the data subject's explicit **consent**.

5.3. Oakswood College will identify and record at least one lawful basis for each processing activity and will only rely on consent where it can be shown that consent is freely given, specific, informed and unambiguous, and where individuals can withdraw consent easily at any time.

5.4. Where Oakswood College relies on **legitimate interests** as its lawful basis, it will carry out a **Legitimate Interests Assessment (LIA)** to document:

- the legitimate interest being pursued
- the necessity of the processing for that purpose
- the balancing of those interests against the rights and freedoms of the individuals concerned, including any safeguards or mitigation measures.

5.5. The outcome of LIAs will be recorded and kept under review, particularly if the nature, scope or context of the processing changes.

5.6. Oakswood College will only rely on **consent** where it can be shown that consent is freely given, specific, informed and unambiguous, and where individuals can withdraw consent easily at any time.

5.7. **Special Category Data and Criminal Offence Data** will only be processed where an appropriate lawful basis applies and an additional condition for processing such data is satisfied (for example explicit consent or a condition set out in the Data Protection Act 2018. The relevant condition will be documented and reflected in the applicable privacy notice.

6. TRANSPARENCY

6.1. Oakswood College will provide clear and accessible information to individuals about how their personal data is used by means of privacy notices and other communications. Privacy notices will be written in plain language, tailored to the audience and easily available at the point data is collected or as soon as reasonably practicable afterwards.

7. PURPOSE LIMITATION

7.1. Personal data will only be collected for specific, explicit and legitimate purposes, and will not be used in a way that is incompatible with those purposes.

7.2. If Oakswood College wishes to use personal data for a new purpose that is different from, but compatible with, the original purpose, individuals will be informed and any additional legal requirements will be met.

7.3 Where the new purpose is incompatible, fresh consent or another appropriate lawful basis will be obtained before processing.

8. DATA MINIMISATION

8.1. Oakswood College will only collect and retain the minimum amount of personal data needed to fulfil the stated purposes. Staff must not collect personal data "just in case" it might be useful in future.

8.2. Forms, systems and processes will be designed to avoid collecting unnecessary data. Existing data collections should be reviewed periodically to ensure that all fields and categories remain necessary and proportionate.

9. ACCURACY

9.1. Personal data must be accurate and, where necessary, kept up to date. Oakswood College will take reasonable steps to check the accuracy of data at the point of collection and at appropriate intervals afterwards.

9.2. Inaccurate or incomplete data will be rectified or erased without undue delay once identified, taking into account legal obligations and the context in which the data is used.

10. STORAGE LIMITATION AND DATA RETENTION

10.1. Personal data must not be kept for longer than is needed for the purposes for which it was collected. When data is no longer required, it will be securely destroyed, erased or anonymised, in line with Oakswood College's Data Retention Policy and Retention Schedule.

10.2. Oakswood College will maintain a Data Retention Schedule setting out standard retention periods for key categories of personal data, including staff, student, applicant, alumni, customer and supplier records, taking into account legal, regulatory, contractual, professional and sector-specific requirements (including the requirements of the Office for Students (OfS) where applicable).

10.3. In relation to students' assessed work and associated assessment records (including examination scripts, coursework submissions, feedback, marks, moderation documentation and assessment or exam board records), Oakswood College will retain such information for long enough to:

- complete internal and external quality assurance processes
- enable the handling of appeals, complaints, cases falling within the scope of the Policy on Sexual Misconduct, Harassment & Unacceptable Behaviours, Support

Through Studies and academic misconduct cases, and any other cases such as arise under any institutional student-related procedures

- demonstrate compliance with relevant OfS ongoing conditions of registration, particularly the conditions relating to academic standards and the quality of courses (the B conditions).

10.4. To meet these requirements, Oakswood College will retain a proportionate sample of students' assessed work and related assessment records for a minimum period of five years after the student has completed or left the course, or for any longer period required to meet OfS expectations, professional or statutory body requirements, or other legal or regulatory obligations.

10.5. At the end of the applicable retention period, students' assessed work and related assessment records will be securely destroyed or anonymised so that individual students can no longer be identified, unless a longer retention period is properly justified and documented (for example, because of ongoing legal or regulatory proceedings).

11. SECURITY, INTEGRITY AND CONFIDENTIALITY

11.1. Oakswood College will implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

11.2. Security measures will be proportionate to the nature, sensitivity and volume of the personal data and may include, for example, access controls, encryption, pseudonymisation, secure configurations, physical security, back-up and recovery arrangements, and regular monitoring and testing.

11.3. Staff must follow all information security policies and procedures, use only approved systems and storage locations, keep passwords secure, and take care when sharing or transmitting personal data.

11.4. Data security encompasses:

- confidentiality (ensuring that only authorised individuals have access to the data)
- integrity (ensuring that data is accurate, complete and reliable for its intended use)
- availability (ensuring that authorised users can access the data when required for legitimate purposes).

11.5. Failure to comply with data security requirements may result in disciplinary action and, where appropriate, may also have legal consequences.

12. INTERNATIONAL TRANSFERS (TRANSFER LIMITATION)

12.1. Personal data will not be transferred outside the UK/EEA unless appropriate safeguards are in place and the transfer complies with data protection law. This may include the use of standard contractual clauses, international data transfer agreements, adequacy regulations or other approved mechanisms.

12.2. Staff must not store or transfer personal data using services or systems that involve international transfers unless those services have been assessed and approved in line with Oakswood College's information governance and procurement processes.

13. DATA SUBJECT RIGHTS AND REQUESTS

13.1. Individuals have a range of rights in relation to their personal data. These rights apply in specific circumstances and include:

- the right to be informed about how their data is used
- the right of access to their personal data
- the right to have inaccurate data corrected (rectification)
- the right to have personal data erased in certain situations (erasure)
- the right to restrict processing in certain situations
- the right to data portability, enabling them to obtain and reuse their data in a structured, commonly used and machine-readable format
- the right to object to certain types of processing (for example direct marketing or processing based on legitimate interests)
- rights related to automated decision-making and profiling
- the right to withdraw consent where consent is the lawful basis for processing
- the right to be notified of certain personal data breaches that are likely to result in a high risk to their rights and freedoms
- the right to lodge a complaint with the Head of GQC & IS

13.2. Requests from individuals to exercise any of these rights, including requests for access to personal data (subject access requests), must be handled promptly and in line with legal timescales and internal procedures. Subject Access Requests must be responded to without undue delay and within one month of receiving the request (or from the day Oakswood College receives any information it reasonably needs to confirm the requester's identity or clarify scope).

13.3. Staff who receive a written or verbal request relating to personal data must forward it without delay to the Head of GQC & IS and must not respond substantively unless authorised to do so.

13.4. Please see Annex 1: Subject Access Request Protocol at the end of this Policy for the procedures that must be followed in the event of a Subject Access Request or similar request received.

14. AUTOMATED PROCESSING AND AUTOMATED DECISION‑MAKING (ADM)

14.1. Where Oakswood College uses profiling or automated decision-making that produces legal effects concerning an individual or similarly significantly affects them, additional safeguards will be applied in line with data protection law.

14.2. Any proposals for new or changed profiling or ADM activities must be referred to the Head of GQC & IS before implementation and may require a data protection impact assessment.

14.3. Individuals affected by qualifying ADM will normally be given meaningful information about the logic involved, the significance and envisaged consequences of the processing, and the opportunity to obtain human intervention, express their point of view and, where appropriate, contest the decision.

15. DIRECT MARKETING

15.1. Oakswood College will comply with data protection and e-privacy requirements when carrying out direct marketing activities, including email, SMS, telephone and postal marketing.

15.2. Appropriate consent or other lawful bases will be used for marketing, and individuals' marketing preferences will be respected and recorded. Opt-out mechanisms will be simple and effective.

15.3. Staff must follow Oakswood College's direct marketing and communications procedures and must not use personal data for unsolicited marketing outside these arrangements.

16. PERSONAL DATA BREACHES AND NOTIFICATION

16.1. A personal data breach may occur through, for example, loss or theft of devices or documents, mis-directed emails, unauthorised access to systems, accidental disclosure or alteration of data, or technical failures that compromise security.

16.2. All suspected or actual personal data breaches must be reported immediately to the Head of GQC & IS using Oakswood College's incident reporting process. Staff must not

attempt to investigate incidents themselves beyond taking immediate steps to contain any obvious risk, and they must preserve any evidence that may be needed.

16.3. Oakswood College will assess reported incidents promptly to determine whether a personal data breach has occurred, the likely impact on individuals, and whether the breach must be notified to the Head of GQC & IS and, where appropriate, to affected individuals or the wider public.

16.4. Where a notifiable breach is likely to result in a risk to the rights and freedoms of individuals, Oakswood College will report it to the Head of GQC & IS without undue delay and, where feasible, within 72 hours of becoming aware of it. Affected individuals will be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

17. TRAINING AND AWARENESS

17.1. All new staff will receive basic data protection and information security training as part of their induction.

17.2. Refresher training and targeted guidance will be provided periodically so that staff remain aware of their responsibilities and understand how to handle personal data securely and lawfully in their roles.

17.3. Failure to complete mandatory training or to follow the requirements of this policy may be treated as a disciplinary issue.

18. RECORDS AND DOCUMENTATION

18.1. Oakswood College will maintain appropriate records of its data processing activities, including Records of Processing Activities (RoPA), data sharing arrangements, data protection impact assessments (DPIAs), Legitimate Interests Assessments (LIAs), retention schedules and security measures, as required by UK GDPR and associated guidance.

18.2. DPIAs will be carried out for processing activities that are likely to result in a high risk to individuals' rights and freedoms, such as large-scale processing of sensitive data, systematic monitoring, or new technologies. The outcomes of DPIAs, including any mitigating measures, will be documented and monitored.

18.3. LIAs will be undertaken and documented whenever Oakswood College relies on legitimate interests as a lawful basis, to ensure that those interests are balanced appropriately against individuals' rights and expectations.

18.4. These records and assessments will be reviewed and updated when processing activities, associated risks, or applicable legal and regulatory requirements change.

19. MONITORING AND REVIEW

19.1. This policy and related procedures will be reviewed at regular intervals, and whenever there are significant changes to law, regulation, guidance or Oakswood College's activities, to ensure that they remain effective and appropriate.

19.2. Updates to the policy will be approved through Oakswood College's governance processes and communicated to staff and other relevant stakeholders.

Oakswood College
Empowering Through Education

APPENDIX 1: Subject Access Request Protocol

The following protocol should be followed by Oakswood College in the event of receiving a Subject Access Request (SAR):

1. Receipt and logging

a) All SARs (email, letter or form) are forwarded immediately to the Head of GQC & IS, who will follow the steps below:

b) The request is logged with:
   - date received
   - requester's details
   - scope of request, and
   - allocated handler.

c) An acknowledgement is sent by the Head of GQC & IS or their nominee within 5 working days, explaining the normal one-month deadline and requesting ID/clarification if needed.

2. Verify identity and clarify scope

a) Where necessary, request reasonable proof of identity and any clarification needed to narrow the request (e.g. dates, systems, types of records).

NOTE: The statutory one-month timeframe runs from receipt of the SAR, or from receipt of ID/clarification if that is required.

3. Locate and collect information

a) Notify relevant areas (e.g. registry, academic departments, HR, IT) of the SAR and the search parameters.

b) Ask them to search all relevant systems and files (email, student record system, VLE, HR files, shared drives) and return results to the Head of GQC & IS by an internal deadline.

4. Review and (where strictly necessary) redact

a) Review the collated information to:

b) remove duplicates and irrelevant material

c) redact third-party data where consent is not available or disclosure would be unreasonable

d) withhold any information falling under an exemption (e.g. legal privilege), recording the rationale.

5. Prepare and issue the response

a) Provide the requester with:
b) a copy of their personal data in an accessible format
c) an explanation of the purposes of processing, lawful bases, categories of data, recipients, retention and their rights.
d) Aim to send the response well within one month; where the request is complex, agree any extension (up to a further two months) with the Head of GQC & IS , notify the requester within the first month, and explain the reasons.

6. Record-keeping and follow-up

a) Record the outcome, date of response, any exemptions applied and any extension used.

b) Note any learning points or process improvements and, where necessary, update internal guidance or staff training.