# DATA PROTECTION POLICY AND PROCEDURE FOR STAFF AND STUDENTS (GDPR)

March 2026

| | |
|---|---|
| **Policy Name and Number:** | Data Protection Policy and Procedure for Staff and Students (GDPR) - 05 |
| **Version** | V4 |
| **Approved by and date:** | Corporation – 25 March 2026 |
| **SLT Lead:** | Data Protection Officer |
| **a. Responsible Manager for policy review:**<br>**b. Responsible Manager for policy implementation (if different):** | Data Protection Officer |
| **How does the policy link to the Strategic Plan Aims and Themes:**<br>**Aims**:<br>*1. Outstanding Teaching, Learning and Assessment*<br>*2. Beneficial Partnerships*<br>*3. Sustainable SMART Campuses*<br>*4. Inclusive, Thriving Community*<br>*5. Financial Sustainability*<br>**Themes:**<br>*a. Sustainability and the environment*<br>*b. Happiness and wellbeing*<br>*c. Digital transformation*<br>*d. Equality, diversity and inclusion* | Continue to develop our estate so that it is recognised as world class in terms of quality, sustainability and the promotion and practice of evolving leading-edge technologies. |
| **a. Related Policies and Procedures:**<br>**b. Related Legislation:** | a:<br>- Data Breach Notification<br>- Rights of Individuals<br>- Privacy Statement<br>b:<br>- GDPR<br>- Data Protection Act<br>- Privacy and Electronic Communications Regulations |
| **Consultation Process:** | Exec - 2 December 2025<br>EIC - 12 February 2026<br>Corporation – 25 March 2026 |
| **Approving Authority:** | SLT Approval ☒<br>Corporation Approval ☒ |
| **Policy Review Frequency:** | Yearly |
| **Effective Date:** | 25 March 2026 |
| **Date of Next Revision:** | 24 March 2027 |
| **Scope:** | Staff: ☒<br>Students: ☒<br>Stakeholders: ☒<br>Visitors: ☒<br>Volunteers: ☒<br>Contractors: ☒ |

| Policy classification: | **Public** (website): ☐<br><br>**Internal**:<br>SharePoint ☒<br>Governor Portal ☒<br>Canvas ☒ |
|---|---|

## 1. Introduction

Oaklands College is committed to ensuring the protection and security of all personal data we hold in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy sets out how we handle personal data, including safeguarding information, to ensure that it is processed lawfully, fairly, and transparently.

## 2. College Vision, Mission, KPIs and Objectives

2.1 **Vision**: To be a sustainable educational trailblazer inspiring our learners and our wider community to achieve their potential in a changing world.

2.2 **Mission**: To prepare every learner for work, a rewarding career, and life's opportunities. By treating every student as the individual they are, with care, passion and understanding in a professional, contemporary and community-focused environment they'll value and enjoy.

2.3 This policy aligns with **Strategic Aim 3:**

Continue to develop our estate so that it is recognised as world class in terms of quality, sustainability and the promotion and practice of evolving leading-edge technologies.

This policy also aligns with **Strategic Objectives:**

b) Create a digitally SMART campus through embracing current and future technologies and industry best practice

c) Effectively manage the estate to model best practice of regulatory compliance

## 3. Purpose

This is the College's overarching policy in relation to data protection.

## 4. Scope of this Policy

This policy applies to all staff and governors.

## 5. College Vision, Mission, Values and Themes

Data protection is a legal requirement which underpins all of the College's strategic ambitions and activities.

## 6. Link to Key Strategic Aims & Objectives

Strategic aims and objectives related to digital transformation and our community our most applicable.

## 7. Policy Statement

We are committed to protecting the privacy and security of personal data relating to students, parents, staff, and third parties. We collect, process, and store personal data only where it is necessary to fulfil our responsibilities as an educational institution. All personal data is handled lawfully, fairly, and transparently, in accordance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. We implement robust measures to safeguard personal information and regularly review our practices to ensure ongoing compliance with data protection principles.

## 8. Monitoring Impact

Impact is monitored at the Information Governance Group meetings and reported to the Estates and Infrastructure Committee.

## 9. Data Protection Principles

We adhere to the following principles when processing personal data:

a) Lawfulness, Fairness, and Transparency: Personal data will be processed lawfully, fairly, and in a transparent manner.
b) Purpose Limitation: Data will be collected for specified, explicit, and legitimate purposes and not processed further in a manner incompatible with those purposes.
c) Data Minimisation: We will only collect data that is adequate, relevant, and limited to what is necessary for the purposes of processing.
d) Accuracy: Personal data will be kept accurate and, where necessary, up to date.
e) Storage Limitation: Data will be retained only for as long as necessary for the purposes for which it is processed, in line with our retention policy.
f) Integrity and Confidentiality: We will ensure appropriate security of personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage, by implementing appropriate technical and organisational measures.
g) Accountability: We are responsible for ensuring compliance with these principles and will be able to demonstrate this compliance.

## 10. Handling of Personal Data – Staff Procedures

### 10.1. Obtaining data

a. When obtaining personal data, it is essential to ensure that individuals are not deceived or misled about the purposes for which their data will be held, used, or disclosed. Transparency is key to maintaining trust and compliance with data protection principles.

b. Additionally, personal data must be collected without applying any unfair pressure or coercion. Individuals should provide their information freely and with a clear understanding of how it will be processed.

c. It must be ensured that personal data is obtained and processed for a specified lawful purpose. The GDPR provides the following lawful bases (GDPR Article 6):

   i. the Data Subject has given his or her Consent (must be freely obtained with clear, affirmative action);
   ii. the Processing is necessary for the performance of a contract with the Data Subject;
   iii. to meet our legal compliance obligations;
   iv. to protect the Data Subject's vital interests;
   v. Processing is necessary for performing a task carried out in the public interest or in the exercise of official authority (e.g., public health initiatives by government bodies)
   vi. to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices. Contact the DPO before relying on legitimate interest.

d. All forms used to collect data must indicate the purpose(s) as well as: the lawful basis for processing the data, the data retention period and that individuals have the right to complain to the ICO if they think there is a problem with the way the data is being handled.

e. The Data Protection Officer (DPO) must be consulted prior to the implementation of any new system, software, or process that involves the processing of personal data. If the DPO determines that the processing is likely to pose a high risk to the rights and freedoms of individuals, a Data Protection Impact Assessment (DPIA) (see appendix 1) will be required. Additionally, the DPO will assess and confirm whether the terms, conditions, and clauses of any new contract are adequate from a data protection standpoint.

### 10.2 Access & holding data

a. Access to and storage of personal data must be strictly controlled to maintain security and confidentiality. Only authorized users should access systems containing personal data, using individual passwords and secure authentication methods. Computers must be locked or logged off when not in use, and areas containing personal data - whether electronic or manual - should be secured at all times. Any holding of College related information outside the College must comply with agreed restrictions, and procedures should be in place to prevent unauthorized access or accidental disclosure.

b. Additionally, robust measures must be implemented to ensure personal data is not disclosed intentionally or inadvertently. This includes clear protocols for handling data, regular staff training, and monitoring compliance. All users share responsibility for safeguarding information and must follow established security practices to protect against breaches.

### 10.3 Disclosing data

Before disclosing personal data, it must be clear which legal basis under Articles 6 and 9 is being relied upon, and any sharing with a third party must be recorded in the Third Party Register. Disclosure should only occur after verifying the identity of the requester and, where appropriate, confirming the data subject's consent. Additionally, all transfers of personal data to third parties must be carried out securely, using encryption or pseudonymisation to protect confidentiality and prevent unauthorised access.

### 10.4 Disposal

Personal data is disposed of properly in line with agreed guidance, best practice and regulatory requirements – see data retention policy

## 11. Handling Special Category Data

11.1 In accordance with Article 9 of the UK GDPR, the College recognises that special category data requires stricter controls due to its sensitivity. The UK GDPR defines special category data as:

a) personal data revealing racial or ethnic origin;
b) personal data revealing political opinions;
c) personal data revealing religious or philosophical beliefs;
d) personal data revealing trade union membership;
e) genetic data;
f) biometric data (where used for identification purposes);
g) data concerning health;
h) data concerning a person's sex life; and
i) data concerning a person's sexual orientation.

11.2 The College is committed to processing special category data in a manner that ensures privacy and compliance with legal obligations.

11.3 Special category data can only be processed under specific conditions outlined in Article 9(2) of the GDPR. The College will only process this data when one or more of the following conditions are met:

a) Explicit consent
b) Employment, social security and social protection (if authorised by law)
c) Vital interests
d) Not-for-profit bodies with political, religious or trade unions aims
e) Made public by the data subject
f) Legal claims or judicial acts
g) Reasons of substantial public interest (with a basis in law)
h) Health or social care (with a basis in law)
i) Public health (with a basis in law)
j) Archiving, research and statistics (with a basis in law)

11.4 For all processing of special category data, the College will:

a) Maintain detailed records of the legal basis relied upon for processing.
b) Ensure that Data Protection Impact Assessments (DPIAs) (see appendix 1) are conducted where required, particularly for new or high-risk processing activities involving special category data.

## 12. Subject Access Requests

Please see the Rights of Individuals Policy and Procedure for information

## 13. Data Subject's rights and request

13.1. Data Subjects have rights when it comes to how we handle their Personal Data, including the right to erase their data in general. These include rights to:

a) withdraw consent to processing at any time;
b) receive certain information about the Data Controller's processing activities;
c) request access to their personal data that we hold;
d) prevent our use of their personal data for direct marketing purposes;
e) ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
f) restrict processing in general circumstances;
g) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
h) request a copy of an agreement under which personal data is transferred outside of the EEA;
i) object to decisions based solely on automated processing
j) prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
k) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
l) make a complaint to the supervisory authority; and
m) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

13.2 You must immediately forward any data subject request you receive to the DPO and comply with the company's data subject response process.

## 14. Accountability / Responsibility for Implementation

14.1 The Senior Management Team and the Corporation are responsible for ensuring that data protection systems and procedures are fully implemented, comprehensive, and effective. All College managers must make sure these systems are followed, provide guidance to staff and students on their responsibilities, and ensure that everyone, including themselves, receives regular training on data protection policies.

14.2 Every member of staff and all students share responsibility for complying with data protection procedures and relevant legislation. They must report any breaches or areas for improvement to senior managers. Failure to adhere to these requirements will result in disciplinary action against any College personnel or student who contravenes the procedures.

14.3 Complaints and appeals regarding data protection are made to the Data Protection Officer (DPO) at:

Oaklands College, St Albans Campus, Hatfield Road, St Albans, AL4 0JA or dpo@oaklands.ac.uk

Failure of any member of staff to inform college management of the existence of an information system or a breach involving personal data may result in disciplinary action.

## 15. Oaklands College Data Protection support structure and responsibilities

15.1. Data Protection Officer **-** The College has appointed the Director of Governance as the Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

15.2. Please contact the DPO with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the College)
b) if you need to rely on Consent and/or need to capture Explicit Consent
c) if you need to draft Privacy Notices or Fair Processing Notices
d) if you are unsure about the retention period for the Personal Data being Processed
e) if you are unsure about what security or other measures you need to implement to protect Personal Data
f) if there has been a Personal Data Breach
g) if you are unsure on what basis to transfer Personal Data outside the EEA
h) if you need any assistance dealing with any rights invoked by a Data Subject
i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes others than what it was collected for;
j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making
k) If you need help complying with applicable law when carrying out direct marketing activities
l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors)

15.3. Data Protection Champions have been appointed to support the Data Protection Officer in the implementation and operation of the Data Protection Policy. These are the members of the Information Governance Group. Data Protection Champions are nominated to advise and support staff in meeting their responsibilities.

15.4. The College has established an Information Governance Group (IGG) to oversee and coordinate information governance activities, compliance with relevant data protection laws and regulations, and promote responsible and secure data handling practices throughout the college. The IGG reports to the Senior Leadership Team. Reporting of data protection matters at a Corporation level takes place via the Estates ad Infrastructure Committee.

## 16. Breaches of Data Protection

Please see the Data Breach Policy and Data Breach Procedure for more information.

## 17. List of relevant legislation

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
The Privacy and Electronic Communications Regulations
The Codes of Practice issued by the Information Commissioner.

## 18. Reviewing, monitoring and recording personal data

18.1. The College will:

a) undertake an annual of review of this policy and subject it to College approval
b) undertake regular testing of privacy measures by conducting periodic reviews and audits to assess compliance
c) keep full and accurate records of all data processing activities including:

I. Details of the Data Controller
II. Details of the DPO
III. Clear descriptions of Personal Data types and Data Subject types
IV. Details of personal data that is captured
V. Records of the lawful bases for processing personal data and where this is consent, the procedures for obtaining consent
VI. Details of third-party recipients of Personal Data
VII. Details of Personal Data transfers
VIII. Details of Personal Data retention periods
IX. Description of security measures in place

## 19. Exemptions to the policy

No exemptions

## 20. Method for achieving policy

Staff training and awareness and implementation of the related policies.

## Appendix 1

# DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

### Submitting controller details

| | |
|---|---|
| Name of controller | |
| Subject/title of DPO | |
| Name of controller contact /DPO (delete as appropriate) | |

### Step 1: Identify the need for a DPIA

| |
|---|
| Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. |
| |

### Step 2: Describe the processing

| |
|---|
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
| |

| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
| --- |
| |

| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| --- |
| |

| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly? |
| --- |
| |

### Step 3: Consultation process

| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? |
|---|
| |

### Step 4: Assess necessity and proportionality

| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? |
|---|
| |

### Step 5: Identify and assess risks

| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|---|---|---|---|
| | Remote, possible or probable | Minimal, significant or severe | Low, medium or high |

## Step 6: Identify measures to reduce risk

| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | |
|---|---|---|---|---|
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| | | Eliminated<br>reduced<br>accepted | Low<br>medium<br>high | Yes/no |

## Step 7: Sign off and record outcomes

| **Item** | **Name/position/date** | **Notes** |
|---|---|---|
| Measures approved by: | | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: | | |
| DPO advice accepted or overruled by: | | If overruled, you must explain your reasons |

| | | |
|---|---|---|
| Comments: | | |
| Consultation responses reviewed by: | | If your decision departs from individuals' views, you must explain your reasons |
| Comments: | | |
| This DPIA will kept under review by: | | The DPO should also review ongoing compliance with DPIA |