Strategy, Policy & Procedure – 05

Data Protection Policy and Procedure for Staff and Students (GDPR)

September 2023

STRATEGY, POLICY AND PROCEDURE - 05

1. Policy Statement/Purpose/Introduction

1.1. to process relevant personal data regarding members of College personnel, volunteers, applicants, parents, pupils and their siblings, alumni and customers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

1.2. Oaklands College will comply with Data Protection Legislation through taking specific measures to ensure that all personal data held about data subjects in the files of any information system, electronic or manual, is processed according to the Data Protection Principles.

1.3. This Policy applies to all College Personnel. You must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you in order for the College to comply with applicable law. Your compliance with this Policy is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Policy. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Privacy Standard may result in disciplinary action.

1.4. This Privacy Standard (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

2. Definitions

2.1. Definitions extracted from Article 4 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

2.2. **AUTOMATED DECISION-MAKING (ADM)**: when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

2.3. **AUTOMATED PROCESSING**: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

2.4. **COLLEGE NAME:** Oaklands College ("the College") which includes all affiliates, subsidiaries and joint ventures, namely Oaklands Commercial Ltd and Together Training Ltd.

2.5. **COLLEGE PERSONNEL**: all employees, workers contractors, agency workers, members and others.

2.6. **CONSENT:** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

2.7. **DATA CONTROLLER:** means the body, which determines the purposes and means of the processing of personal data. The College is the Data Controller of all Personal Data relating to College Personnel, volunteers, applicants, parents, pupils and their siblings, alumni and customers.

2.8. **DATA PROCESSOR:** means the body which processes personal data on behalf of the Data Controller

2.9. **DATA SUBJECT:** means a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

2.10. **DATA PROTECTION OFFICER (DPO)**: means the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

2.11. **EEA**: means the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

2.12. **GENERAL DATA PROTECTION REGULATION (GDPR)**: means the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

2.13. **PERSONAL DATA:** means any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal Data specifically includes, but is not limited to:

- Name
- Identification number
- Location data
- Online identifier or
- One or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person

2.14. **PERSONAL DATA BREACH:** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.15. **PRIVACY GUIDELINES:** means the College privacy/GDPR related guidelines provided to assist in interpreting and implementing this Privacy Standard and Related Policies.

2.16. **PRIVACY NOTICES (ALSO REFERRED TO AS FAIR PROCESSING NOTICES) OR PRIVACY POLICIES**: means separate notices setting out information that may be provided to Data Subjects when the College collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

2.17. **PROCESSING:** means any operation which is performed on Personal Data whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.18. **PSEUDONYMISATION:** replacing information that directly or indirectly identifies an individual with one or more artificial identifier or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information, which is meant to be kept separately and secure.

2.19. **SENSITIVE PERSONAL DATA**: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

3. Data Protection Principles

3.1. The Data Protection Principles are:

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Personal data shall not be transferred to another country without appropriate safeguards being in place
- Personal Data shall be made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data

4. Handling of Personal Data – Staff Procedures

4.1. Obtaining data

- Ensure that any person from whom personal data is obtained should not be deceived or misled regarding the purposes for which data is held, used or disclosed.

- No unfair pressure is used to obtain any personal data.
- Ensure that Personal Data is obtained and processed for a specified lawful purpose. The GDPR provides the following lawful bases:
  a) the Data Subject has given his or her Consent;
  b) the Processing is necessary for the performance of a contract with the Data Subject;
  c) to meet our legal compliance obligations;
  d) to protect the Data Subject's vital interests;
  e) 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; or
- Where consent is being used as the lawful basis, consent must be freely obtained from a clear affirmative action. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

4.2. All forms used to collect data – ensure that an indication of the purpose(s) appears on it 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.

4.3 Individuals do have the right to object to the processing of their data, case by case

Access & holding data

- Only authorised access is allowed to information systems containing personal data (e.g. by the use of individual passwords).
- The holding of College related information outside the College is operated within agreed restrictions.
- All users switch off/log off and lock their computers when they are not being used to prevent accidental access by others
- Areas containing personal data information systems (including manual files) are secured when not in use
- Unauthorised access to a personal data information system is prevented
- Develop and implement procedures to seek to ensure personal data is not disclosed either intentionally or accidentally

Disclosing data

- Personal data to which an individual/organisation is entitled is only disclosed after receiving proper identification of the person or organisation requesting the information and where appropriate verifying the data subject’s agreement to disclosure

- Personal data disclosure to third parties takes place through an encryption or pseudonymisation process

Disposal

- Personal data is disposed of properly in line with agreed guidance – see data retention policy

5. Subject Access Requests

5.1. Anyone making a subject access request should provide evidence of their identity or their authority to make the request (e.g. a solicitor acting on behalf of a client will provide a letter of authorisation from the client or assurance that permission has been granted) before the request is actioned. A copy of all requests should be given to the Data Protection Officer for monitoring and reporting purposes.

5.2. The GDPR gives individuals the right to obtain the following: a copy of their own data, the purpose of processing, who the data has been shared with and how long the data will be retained. On receipt of a valid request, the DPO (with the input of the Data Controllers) will respond to the request electronically within one month of the request.

5.3. Requests for information can be made in a variety of formats. However, it would be preferable to request the information in writing to: dpo@oaklands.ac.uk or

Joseph Maggs
Data Protection Officer / Director of Governance
St. Albans (Smallford) Campus
Hatfield Road
St. Albans
AL4 0JA

5.4. A response will normally be made within one month. However, if the request is particularly complex, this may be extended to up to 2 months and a cover fee may be charged.

5.5. In some cases, **a response will be rejected** e.g. where an exemption from the Act legitimately applies; the request is manifestly unfounded or excessive; the data contains data related to third parties who have not provided consent to share. Where a response is rejected the college will inform the person within one month. The college will need to:

- explain to the applicant why they are not releasing information
- inform the applicant of their right to complain to the ICO
- the right of the applicant to pursue the request through judicial remedy

6. Data Protection and Subject Access request for 16 to 18 year olds

6.1. 16 to 18 year olds at the College will be considered to be children under the GDPR. In the first place the college will request the right to process the child's data through the college learning agreement. The college will also seek the consent of the student to share their information with parents, carers, or other appropriate agencies. The learning agreement states:

If you are 18 or under, by signing this learning agreement you are giving the College your consent to stay in touch with your parent/guardian/carer with regard to all aspects of progress on your course of study. If you require more information please refer to our Data Protection Policy.

6.2. With regard to subject access requests, under the GDPR, children have the same rights as adults over their personal data; including the right to access their personal data. The ICO guidance states that it is the child who has a right of access to the information held about them, as opposed to a parent or guardian.

6.3. Before responding to a subject access request for information held about a child, the college will consider whether the child is mature enough to understand their rights. If the college is confident that the child can understand their rights, then the college will respond directly to the child. However, the college may allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

6.4. When considering borderline cases, the college will take into account, among other things:

- the child's level of maturity and their ability to make decisions like this
- the nature of the personal data
- any court orders relating to parental access or responsibility that may apply
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment
- any detriment to the child or young person if individuals with parental responsibility cannot access this information
- any views the child or young person has on whether their parents should have access to information about them

6.5. Therefore, the college will need to consider each situation on a case by case basis.

7. Data Subject's rights and request

7.1. 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:

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold;

- prevent our use of their Personal Data for direct marketing purposes;
- 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;
- restrict Processing in general circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling (ADM);
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- 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.

7.2. You must immediately forward any Data Subject request you receive to the DPO and comply with the company's Data Subject response process.

8. Accountability / Responsibility for Implementation

- The Senior Management Team and the Corporation are accountable for ensuring full implementation of data protection systems and procedures, that they are sufficient and comprehensive
- Nominated College Data Controllers are accountable for the oversight of data protection systems and procedures, to support and advise staff and to alert senior managers to breaches or the need for improvement in data control processes
- All College managers are responsible for ensuring that data protection systems and procedures are being followed and advise staff and students regarding their liabilities
- Managers are responsible to ensure that they themselves and all College Personnel are appropriately informed and regularly trained in Data Protection policies and procedures
- All staff and students have responsibility for implementing College data protection procedures and complying with legislation
- Disciplinary action will be taken against any College Personnel or student who contravenes these procedures
- Complaints and appeals regarding data protection are made to the Data protection officer (DPO) at the Quality Office:

Quality Office, 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 containing personal data may result in disciplinary action.

9. Oaklands College Data Protection support structure and responsibilities

9.1. **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). The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy.

9.2. 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:

- 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)
- if you need to rely on Consent and/or need to capture Explicit Consent
- if you need to draft Privacy Notices or Fair Processing Notices
- if you are unsure about the retention period for the Personal Data being Processed
- if you are unsure about what security or other measures you need to implement to protect Personal Data
- if there has been a Personal Data Breach
- if you are unsure on what basis to transfer Personal Data outside the EEA
- if you need any assistance dealing with any rights invoked by a Data Subject
- 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;
- If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making
- If you need help complying with applicable law when carrying out direct marketing activities
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors)

9.3. **Data Controllers**

Data Controllers 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.

9.4. Data Controllers are nominated to advise and support staff in meeting their responsibilities.

10. Breaches of Data Protection

10.1. Suspected breaches of data should be dealt with in accordance with the College's Data Breach Notification Policy.

10.2. The ICO will be informed where the breach is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

10.3. All queries regarding the processing of data in the first instance are raised with the relevant line manager or lecturer for all staff and students respectively.

10.4. Anyone aware of a potential breach must report it as soon as possible in line with this policy.

10.5. The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

10.6. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

10.7. If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO, or one of the Data Controllers. You should preserve all evidence relating to the potential Personal Data Breach.

10.8. Potential fines for non compliance with GDPR exceed those of the previous data protection regime. The previous maximum was £500,000. Under GDPR the maximum is £20,000,000 or 4% of worldwide annual turnover. Examples of fines imposed by the ICO can be found at https://ico.org.uk/action-weve-taken/enforcement/

10.9. Individuals also have the right to claim compensation through the courts for damages caused by a breach.

11.List of Relevant Legislation

- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
- The Freedom of Information Act 2000
- The Privacy and Electronic Communications Regulations
- The Codes of Practice issued by the Information Commissioner.

12.Reviewing, monitoring, recording personal data

12.1. The College will:

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

STRATEGY, POLICY AND PROCEDURE - 05

a) Details of the Data Controller
b) Details of the DPO
c) Clear descriptions of Personal Data types and Data Subject types
d) Details of personal data that is captured
e) Records of the lawful bases for processing personal data and where this is consent, the procedures for obtaining consent
f) Details of third-party recipients of Personal Data
g) Details of Personal Data transfers
h) Details of Personal Data retention periods
i) Description of security measures in place