



UK GDPR and Data Protection Policy September 2024

Policy reviewed: June 2018

To be next reviewed: November 2025

To be reviewed by: Policy and Procedures Lead, Nikki Twiner

This policy will be reviewed at least annually and/or following any updates to national and local guidance and procedures.

The Oaks Specialist College: UK GDPR and Data Protection Policy

Introduction

This policy sets out the The Oaks Specialist College's commitment to comply with the UK General Data Protection Regulations (GDPR).

The College as the Data Controller will comply with its obligations under the UK GDPR and DPA. The College is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy

Scope of the Policy

The Oaks is required to process relevant personal data regarding members of staff, trustees, volunteers, applicants, learners (both past and present) and their families as part of its normal operation and we shall take all reasonable steps to do so in accordance with this policy, the Data Protection Regulations and GDPR.

The Principles

The principles set out in the UK GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (data minimisation)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (accuracy).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (storage limitation)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information is processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (integrity and confidentiality).

Transfer Limitation

Personal data shall not be transferred to a country outside the UK unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided

explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the UK.

Personal and Sensitive Data

All data within the College shall be identified as personal, sensitive or a combination of both. This will ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of individuals to whom it relates. Personal data covers both facts and opinions about an individual where that data identifies an individual. It includes information necessary for employment such as names, addresses, salary details or attendance records or exam results.

Personal data may also include sensitive personal data.







Sensitive personal data includes data relating to medical information, gender, religion, race, sexual orientation, trade union membership and criminal records.

Processing of Personal and Sensitive Data

Processing data involves the collating, storing, retrieving, consulting, disclosing, sharing, erasing or destroying personal data.

Personal data

As an educational provider The Oaks Specialist College is required to gather, store and share information to a variety of institutions in order for us to carry out our contracts of delivery and every day operation. This may include, but is not exclusive to:

-  Department for Education and other Government Departments
-  Local Authorities
-  Awarding Bodies
-  Health Providers
-  Onward destinations
-  Work placements




Sensitive Data

In the event that the College is required to share sensitive information about a learner or a member of staff, this will only be done so under strict conditions, including gaining expressed permission of the person concerned.

For the avoidance of doubt, The Oaks Specialist College is a post 16 institution, and our learners are over 18. In an event where personal information is required to be shared beyond the realms of our day to day operation, the young person concerned can give consent. This is on the basis that the learner has not undergone a Mental Capacity Assessment which deems them unable to make a decision in this regard. If a young person is not able to provide consent, we will refer the request for consent to an appropriate care provider/giver.

Exemptions

Certain data is exempt from the provision of the Data Protection Act:

-  Information that affects national security and the prevention or detection of crime
-  The assessment of tax or duty
-  Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the College.

Data Storage and Security

Wherever possible information regarding both learners and staff is saved on the College computer drives. There are varying levels of access to information; this is dependent upon on the requirements of job roles within the College and the information required by staff members to allow them to actively and purposefully carry out their roles.

Learner information is saved on the College Learner Database (Databridge). Where hard copies of documents are required, these are kept in locked cabinets and locked rooms within the College.

Sensitive personal information should not be removed from College, however the College acknowledges that some staff may need to transport data between College and their home in order to access it for work purposes. This may also apply in cases where staff have offsite meetings. The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- ✿ Paper copies of data should not be taken offsite. If there is no way to avoid taking a paper copy, the data should not be on view in public places or left unattended under any circumstances.
- ✿ Unwanted paper copies of personal or sensitive data should be shredded. This also refers to handwritten notes if the notes reference any staff member or learner by name.
- ✿ Care must be taken to ensure that any printout of any personal or sensitive data is not left in printer trays or photocopiers.
- ✿ If data is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended.
- ✿ Sensitive data should not be viewed on public computers.
- ✿ If it is necessary to transport data away from College it should be downloaded onto a USB stick (or other suitable secure device). The data should not be transferred from this stick onto any home or public computer
- ✿ USB sticks (or other suitable devices) must be password protected
- ✿ Confidential e-mails should be sent via Egress, wherever possible.

All colleagues are responsible for ensuring that:

- ✿ any personal data that they hold is kept securely
- ✿ Personal information is not disclosed either orally, in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- ✿ They understand the principals of UK GDPR and their responsibilities in this regard.
- ✿ Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe. Staff should also note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Privacy Notice

The College will issue privacy notices as required, informing data subjects (or their parents, depending on mental capacity of the learner, if about learners' information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the UK GDPR including the identity of the DPO, how and why the College will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. The College must also check that the data was collected by the third party in accordance with the UK GDPR and on a basis which is consistent with the proposed processing of the personal data.

The College will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The College will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The College utilises a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Individual Rights

Staff and learners, as well as any other 'data subjects', have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed.
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the College no longer need the personal information, but you require the data to establish, exercise or defend a legal claim.
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the College are verifying whether it is accurate), or where you have objected to the processing (and the College are considering whether the College's legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA.
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers or the public. The College expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not College staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the College's policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the College's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security

The College will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their College's acceptable use policy.

The College will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the College has implemented and maintains in accordance with the UK GDPR and DPA.

Where the College uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the College
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the College and under a written contract
- the organisation will assist the College in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the College as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the College with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the College immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Storage and retention of personal information

Personal data will be kept securely in accordance with the College's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to The Oaks' Retention Schedule for processing personal information.

Personal information that is no longer required will be deleted in accordance with the Colleges Record Retention Schedule.

Data Breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Offences where information is obtained by deceiving the organisation which holds it

The College must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The College must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Principal immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the College's agreed breach reporting process.

Training

The College will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply

Any failure to comply with any part of this policy may lead to disciplinary action under the College's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect. If you have any questions or concerns about this policy, you should contact your line manager or the College's DPO.

Data Protection Officer (DPO)

The person required to be appointed in public authorities under the UK GDPR.

The Oaks Data Protection Officer can be contacted via schools.dpo@eastsussex.gov.uk