



# P003


# DATA PROTECTION POLICY

Approved by Gavin McLean

<b>Issued by</b>	Natasha Varney
<b>Issued date</b>	18/11/2022
<b>Approved Date</b>	18/11/2022
<b>Next Review Date</b>	18/11/2023

## Document Version Control Log

Version	Date	Description of changes
1.1	18/11/2021	
1.2	18/10/2022	Format updated. Published on Hub.
1.3	18/11/2023	Name of principal updated. Introduction of Document Version Control Log.
1.4	18/11/2024	Next scheduled update.

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

## 1. Aims

As an online provider of home education accessible from around the world, Wolsey Hall Oxford is committed to ensuring that the protection of sensitive data and information of its students, student families, and team members is at the heart of what we do. Wolsey Hall Oxford aims to provide a high quality, safe learning experience and is committed to responding appropriately to any concerns of data and privacy breaches.

Wolsey Hall Oxford aims to ensure that all personal data collected about its team members, students, parents, and other individuals is collected, stored, and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format, has the full support of our management team and is communicated to provide a clear understanding of company expectations of team members and associates.


We will review this policy at least annually through our formal Management Review process.

Gavin McLean



Principal

15 November 2023


<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

## 2. Legislation and Guidance

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for Subject Access Requests. It also reflects the ICO's code of practice for the use of personal information.

## 3 Definitions

Term	Definition
<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, individual. This may include the individual's:</p> <ul style="list-style-type: none"> <li>• Name (including initials)</li> <li>• Identification number</li> <li>• Location data</li> <li>• Online identifier, such as a username</li> </ul> <p>It may also include factors specific to the individual's physical, physiological, genetic mental, economic, cultural, or social identity.</p>
<b>Special categories of personal data</b>	<p>Personal data, which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> </ul>
<b>Processing</b>	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
<b>Data Subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data Controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data Processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<b>Personal Data Breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

## 4. The Data Controller

Wolsey Hall Oxford processes personal data relating to parents, students, team members and others, and therefore is a data controller. Wolsey Hall Oxford is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 5. Roles and Responsibilities

This policy applies to all team members employed by Wolsey Hall Oxford, and to external organisations or individuals working on our behalf. Team members who do not comply with this policy may face disciplinary action.

### 5.1 Board of Directors

The board of directors has overall responsibility for ensuring that Wolsey Hall Oxford complies with all relevant data protection obligations.

### 5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and helping to develop related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the board of directors and, where relevant, report to the board their advice and recommendations on data protection issues. The DPO is also the first point of contact for the ICO (Information Commissioner's Office). Full details of the DPO's responsibilities are set out in their SLA (Service Level Agreement). Our DPO is SchoolPro TLC Limited and is contactable via [GDPR@SchoolPro.uk](mailto:GDPR@SchoolPro.uk)


### 5.3 Data Compliance Officer

The Data Compliance Officer (DCO) acts as the representative of the Data Protection Officer on a day-to-day basis. The DCO is also the first point of contact for individuals whose data we process, and for our team members. Should they wish to, team members can directly communicate with the DPO.

### 5.4 All Team Members

Wolsey Hall team members are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy.
- Informing Wolsey Hall Oxford of any changes to their personal data, such as a change of address.
- Contacting the DCO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
  - If they have any concerns that this policy is not being followed.
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
  - If there has been a data breach.

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

- Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
- If they need help with any contracts or sharing personal data with third parties.

## 6. Data Protection Principles

The UK GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.
- This policy sets out how we aim to comply with these principles.

## 7. Collecting Personal Data

### 7.1 Lawfulness, Fairness and Transparency


We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that a public authority can perform a public task and carry out its official functions.
- The data needs to be processed so that Wolsey Hall Oxford can fulfil a contract with the individual, or the individual has asked Wolsey Hall Oxford to take specific steps before entering a contract.
- The data needs to be processed so that Wolsey Hall Oxford can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
- The data needs to be processed for the legitimate interests of Wolsey Hall Oxford or a third party (provided the individual's rights and freedoms are not overridden).
- Where the above does not apply we shall request clear consent from the individual (or their parent/carer when appropriate in the case of a student).

For further detail of which lawful basis is used for each category of data, see the relevant privacy notice.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018. This is laid out in more detail in point 7.3.

As an online home-schooling college, our educational offer relies on the provision of online services to students, such as the provision of our online learning platform in combination with online learning apps. Where this online offer is concerned, we intend, where appropriate, to rely on Public Task or

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

other legal bases as a basis for processing. Where this is not appropriate, we will seek parental consent for processing (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

## 7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Team members must only process personal data where it is necessary in order to do their jobs.

When team members no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with our record retention policy, which can be made available on request.

## 7.3 Our processing of special categories of personal data and criminal offence data

As part of our statutory functions, we process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

### Special Category Data

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:


- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data for the purpose of uniquely identifying a natural person.
- Data concerning health, or
- Data concerning a natural person's sex life or sexual orientation.

### Criminal Conviction Data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data.'

### Appropriate Policy Document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

This section of our Data Protection Policy document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document is not a specific requirement. The information supplements our privacy notices.

#### Conditions for processing special category and criminal offence data

We process special categories of personal data under the following UK GDPR Articles:

**i. Article 9(2)(a) – explicit consent.**

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include team members’ and students’ financial information as well as health information we receive from our students who require a reasonable adjustment to access our services.

**ii. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on our organisation or the data subject in connection with employment, social security, or social protection.**

Examples of our processing include team members’ sickness absences.

**iii. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.**

An example of our processing would be using health information about a student or team member in a medical situation.

**iv. Article 9(2)(f) – for the establishment, exercise, or defence of legal claims.**

Examples of our processing include processing relating to any employment tribunal or other litigation.

**v. Article 9(2)(g) - reasons of substantial public interest.**


As a home-schooling organisation, we are a privately funded body and provide a safeguarding role to young and vulnerable people (See our Safeguarding Policy of January 2021). Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role.

Examples of our processing include the information we seek or receive as part of investigating an allegation.

**vi. Article 9(2)(j) – for archiving purposes in the public or in our interest.**

The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – archiving. For example, archiving student videos relating to home-schooling life at Wolsey Hall Oxford etc.

We process criminal offence data under Article 10 of the UK GDPR.

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

#### Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security, and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for Wolsey Hall Oxford. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. Our retention with respect to this data is documented in our retention schedules, which can be presented upon request.

#### Description of data processed

We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs, and their membership of any union. Further information about this processing can be found in our team members' privacy notice.

We process the special category data about our students and other members of our community that is necessary to fulfil our obligations as a home-schooling organisation, and for safeguarding and care. This includes information about their health and wellbeing, ethnicity, photographs, and other categories of data relevant to the provision of care. Further information about this processing can be found in our student privacy notice.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

### Schedule 1

#### *Conditions for processing Special category data*

We process SC data for the following purposes in Part 1 of Schedule 1:

- Paragraph 1(1) employment, social security, and social protection.

We process SC data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:


- Paragraph 6(1) and (2)(a) statutory, etc. purposes
- Paragraph 18(1) – safeguarding of children and of individuals at risk.

#### *Criminal offence data*

We process criminal offence data for the following purposes in parts 1, 2 and 3 of Schedule 1:

- Paragraph 1 – employment, social security, and social protection.
- Paragraph 6(2)(a) – statutory, etc. purposes.
- Paragraph 12(1) – regulatory requirements relating to unlawful acts and dishonesty etc.
- Paragraph 18(1) – safeguarding of children and of individuals at risk.
- Paragraph 36 – Extension of conditions in part 2 of this Schedule referring to substantial public interest.



<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

## 8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student or parent/carer that puts the safety of our team members at risk.
- We need to liaise with other agencies – we may seek consent, if necessary, before doing this.
- Our suppliers or contractors need data to enable us to provide services to our team members and students – for example, IT and communication companies, education support companies, and those that provide tools for learning. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, if personal data is sufficiently anonymised, or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or team members.


Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## 9. Subject Access Requests and Other Rights of Individuals

### 9.1 Subject Access Requests (SARs)

Individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that Wolsey Hall Oxford holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period.

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter or email to the DCO of Wolsey Hall Oxford, who will then forward to the DPO. They should include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

If team members receive a subject access request, they must immediately forward it to the DCO, who will then forward to the DPO.

## 9.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at Wolsey Hall Oxford may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.


## 9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide two forms of identification.
- May contact the individual via telephone or email to confirm the request was made.
- Will respond without delay and within one month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.


The UK GDPR does not prevent a data subject making a subject access request via a third party. Requests from third parties are dealt with as follows:

- In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the data subject.
- It is the third party's responsibility to provide evidence of this entitlement.
- This might be a written authority to make the request, or it might be a more general power of attorney.
- If there is no evidence that the third party is authorised to act on behalf of the data subject, we are not required to respond to the SAR.
- However, if we are able to contact the data subject, we will respond to them directly to confirm whether they wish to make a SAR.

#### 9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time, where consent is the basis for processing.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly-used and machine-readable format (in certain circumstances).

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

Individuals should submit any request to exercise these rights to the DCO or DPO. If team members receive such a request, they must immediately forward it to the DCO who will then forward it to the DPO.

It is important to note that Wolsey Hall Oxford could be reported to the Information Commissioner's Office (ICO) for failing to comply with our statutory responsibilities regarding SARs and other data protection rights of the individual, and penalties (including financial) may apply.

## 11. Parental Requests to see the Educational Record

There is no legal right for parents, or those with a parental responsibility, to access their child's educational record if the child attends an independent educational institution in England; however, Wolsey Hall Oxford has made the decision to grant access to the parents of our students in line with the ICO's guidance, in order to retain appropriate and regular communication between parents and the school.

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

## 12. Biometric Recognition Systems

Wolsey Hall Oxford does not collect or otherwise process biometric data.

## 13. Photographs and Videos

As part of Wolsey Hall Oxford's activities, we may record images of individuals. No images in any format will be circulated or stored involving students under 18 without the explicit written informed consent of those involved and their parents/guardians/carers.

We will obtain written consent from parents/guardians/carers for photographs and videos to be shared of their child for communication, marketing, and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and student.


Uses may include:

- Within the online setting, on the online community group, emails, website, social media, in brochures, newsletters, etc.
- Outside of Wolsey Hall Oxford by external agencies such as campaigns.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not usually accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Safeguarding Policy for more information on our use of photographs and videos.

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

## 14. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DCO and DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing Data Protection Impact Assessments (DPIAs) where Wolsey Hall Oxford's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process – see section 14.1).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training Wolsey Hall Oxford team members on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our organisation, DCO and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

### 14.1 Data Protection Impact Assessments (DPIAs)


A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project.

We will do a DPIA for processing that is likely to result in a high risk to individuals as well as any other major project which requires the processing of personal data.

It is vital that the DPIA is completed before processing is commenced to ensure that all risks are identified and mitigated as much as possible.

Our DPIA will:

- describe the nature, scope, context, and purposes of the processing;
- assess necessity, proportionality, and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

To assess the level of risk, we will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We will consult our Data Protection Officer (SchoolPro TLC Ltd) and, where appropriate, individuals and relevant experts. We may also need to consult with relevant processors.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

We will implement the measures we identified from the DPIA, and integrate them into our policies, procedures, and practice.

## 15. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage.


In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data should be kept under lock and key when not in use.
- Papers containing confidential personal data must not be left anywhere where there is general access.
- Passwords that are 6 digit (for I-Pad users) or 8 characters long containing letters and numbers are used to access computers, laptops, and other electronic devices. Team members and students are reminded to change their passwords at regular intervals. I-Pad users can also use their tablet's face recognition software.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Team members, students or directors who store personal information on their personal devices should follow the same security procedures as for company-owned IT systems (see our Acceptable Use Policy, which can be presented upon request).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8 – Sharing Personal Data).

## 16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		

## 17. Personal Data Breaches

We will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in the Personal Data Breach Procedure (PR001).

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in our context may include, but are not limited to:

- A non-anonymised dataset being published on our website which shows the exam results of students eligible for the student premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a laptop containing non-encrypted personal data about students.

It is important to note that Wolsley Hall Oxford could be reported to the Information Commissioner's Office (ICO) for high-risk data breaches and penalties (including financial) may apply.

## 18. Training

All team members and directors will be provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or our processes make it necessary.

## 19. Monitoring Arrangements

This policy will be reviewed and updated at least once every year and shared with the board of directors.


## 20. Links with Other Policies

This Data Protection Policy is linked to our:

- Privacy Notice – website
- Privacy Policies
- Safeguarding Policy
- Data Retention Policy
- Acceptable Use Policy

## 21. Links with Procedures

On finding or causing a breach, or potential breach, the team member or data processor must immediately notify the Data Compliance Officer (DCO), triggering the Personal Data Breach Procedure (PR001).

<b>Document</b>	P003 Data Protection Policy	
<b>Revision</b>	1	
<b>Revision Date</b>	18/11/2022	
<b>Created By</b>		