



Policy No: 5a(1)

OUR LADY'S ABINGDON (OLA) DATA PROTECTION POLICY

This policy applies to the whole school; those employed to teach or otherwise engaged to work or volunteer at Our Lady's Abingdon. This policy is publicly available on the school website and upon request a copy (which can be made available in large print or other accessible format if required) may be obtained from the School Office.

Document Details

Information Sharing Category	Public Domain
Version	2
Date Published	September 2021
Authorised by (if required)	Head, Chief Operating Officer, Board of Governors
Review/Update Date	September 2022
Responsible Area	Chief Operating Officer


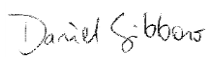

Amendments:

Date	Amendment
October 2020	All policies and associated procedures have been fully revised as of October 2020
September 2021	Reviewed in September 2021

We comply with the Government guidance and regulations, currently in force, regarding COVID.

Monitoring and Review: This policy is subject to continuous monitoring, refinement and audit by the Head and the Chief Operating Officer. The Board of Governors will undertake a full annual review of this policy and procedures, inclusive of its implementation and the efficiency with which the related duties have been discharged. This discussion will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay.

Date Reviewed: September 2021

Chief Operating Officer	Head	Chair of Governors
Prav Karian	Mr Daniel Gibbons	Freddy El Turk
Signed: 	Signed: 	Signed: 

This policy will be reviewed no later than September 2022 or earlier if changes in legislation, regulatory requirements or best practice guidelines so require.

The Designated Data Protection Officer for Our Lady's Abingdon is Prav Karian (Chief Operating Officer) who can be contacted on: 01235 544800.

Related documents:

OLA's Confidentiality and Information Sharing Policy and Online Safety Policy

Privacy notice for pupils

Photography, Filming and Use of images Policy

Our Lady's Abingdon (OLA) is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.

Data Protection Policy: Reviewed September 2021

Contents

1. Aims.....	2
2. Legislation and guidance	2
3. Definitions	3
4. The data controller	3
5. Roles and responsibilities	3
6. Data protection principles.....	4
7. Collecting personal data	4
8. Limitation, Minimisation and Accuracy.....	5
9. Sharing personal data.....	5
10. Subject access requests and other rights of individuals.....	5
11. Other data protection rights of the individual.....	6
12. Parental requests to see the educational record	7
13. Photographs and videos	7
14. Data protection by design and default.....	7
15. Data security and storage of records	7
16. Disposal of records	8
17. Personal data breaches	8
18. Training.....	8
19. Monitoring arrangements	8
20. Links with other policies	8
Appendix 1: Personal data breach procedure.....	9

1. Aims:

OLA aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) on the [GDPR](#) and the ICO’s [code of practice for subject access requests](#).

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data. It also reflects the ICO’s [code of practice](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child’s educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	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.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data. In our case this is in the person of our lead proprietor.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

OLA processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. OLA, through our proprietor, 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 staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Our Lady's Abingdon is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.

Proprietor

The Proprietor is the Governing Board and as such are responsible for ensuring that OLA complies with all relevant data protection obligations.

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 developing related policies and guidelines where applicable. In OLA, the DPO is Prav Karian (Chief Operating Officer).

Reporting to the Board of Governors

The DPO will provide an annual report of their activities to the Board of Governors in the summer term and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Details of the DPO's responsibilities are set out in their job description.

All staff

Staff are responsible for:

- collecting, storing and processing any personal data in accordance with this policy;
- informing the school of any changes to their personal data, such as a change of address;
- contacting the DPO 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, or deal with data protection rights invoked by an individual;
 - if there has been a data breach – refer to OLA's Data Breach Procedure;
 - whenever they are engaging in a new activity that may affect the privacy rights of individuals and if they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The GDPR is based on data protection principles with which OLA must comply. These principles state 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 and in a way that ensures it is appropriately secure.

This policy sets out how OLAI aims to comply with these principles.

7. Collecting personal data

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 the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school 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 so that the school, as a public licensed body, can perform a task **in the public interest**, and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden).

Our Lady's Abingdon is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018. If we offer online services to pupils, such as classroom or subject apps which require use of personal data, and we intend to rely on consent as a basis for processing, we will get parental consent for our pupils who are under 13. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

8. 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. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

9. Sharing personal data

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

- there is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- we need to liaise with other agencies – we will seek consent as necessary before doing this;
- our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies.

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 and
- research and statistical purposes, as long as 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 pupils or staff. Where we transfer personal data to a country or territory we will do so in accordance with data protection law.

10. Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that OLA 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 isn't possible, the criteria used to determine this period;
- the source of the data, if not the individual;

Our Lady's Abingdon is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.

- 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 DPO. They should include:

- name of individual;
- correspondence address;
- contact number and email address and
- details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child. However, we would expect parents to share the ownership of their children's data.

Responding to subject access requests

When responding to requests, we:

- may ask the individual to provide 2 forms of identification;
- may contact the individual via phone to confirm the request was made;
- will respond without delay and within 1 month of receipt of the request;
- will provide the information free of charge;
- may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous.
- we will inform the individual of this within 1 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 pupil 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;
- 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.

11. 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;
- 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;
- 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).

Our Lady's Abingdon is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Requests for data disclosure:

OLA may receive requests from third parties to disclose personal data it holds about pupils, their parents or guardians. OLA confirms that it will not generally disclose information unless the individual has given consent or one of the specific exemptions under the Data Protection Act applies. However, OLA does intend to disclose such data as is necessary to third parties for the following reasons:

- to give a confidential reference.
- to give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend.
- to publish results of public examinations or other achievements.
- to disclose details of a pupil's medical condition where it is in the pupil's interest to do so, e.g. organisers of school trips.

Where OLA receives a disclosure request from a third party, it will take reasonable steps to verify the identity of that third party before making any disclosure.

12. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

13. Photographs and videos *(See also OLA's Photography, Filming and Use of images Policy)*

As part of our school activities, we may take photographs and record images of individuals within OLA.

We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to the parent/carer. Uses may include:

- within OLA on notice boards, school posters, prospectus and newsletters, etc.;
- outside of school by external agencies such as the school photographer, newspapers, campaigns;
- online on our school website or social media pages

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 accompany them with any other personal information about the child, beyond the first name, where necessary to ensure they cannot be identified.

14. Data protection by design and default

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

- appointing a suitably qualified 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 privacy impact assessments where OLA'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);
- integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Regularly training members of staff 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 OLA 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

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 are kept under lock and key when not in use or are password protected;
- papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- where personal information needs to be taken off site it must be safeguarded, papers should be carried in locked bags or cases. The use by staff of removable media eg USB sticks is not permitted, unless password protected;
- passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices;
- staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our *Online safety policy* and *Acceptable use agreements*);
- 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).

Data held electronically:

Personal data is held on the OLA network within our secure databases. All confidential data held on staff, pupils and parents is restricted to key individuals and requires a user name and password for access. Access to folders on the network is also restricted by the Network and our IT Support. Files that contain confidential personal information are password-protected. Data on individuals which OLA would like to feature on the School website will not be posted to the site without parental permission. Access to confidential data is restricted to a minimum number of people.

Hard copy data

Personal data on pupils is held in lockable filing cabinets by the users. Personal data on staff is kept in the Personnel files held in the COO and HR office. Personal data on parents which is held by the School is kept secure by the COO. Access to confidential data is restricted to a minimum number of people.

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 OLA's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

OLA 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 *Data Breach Procedure* attached to this Policy.

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

- a non-anonymised dataset being published on the school website;
- safeguarding information being made available to an unauthorised person;
- the theft of a school laptop containing personal data about pupils.

18. Training

All staff and governors are 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 OLA's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every year** by the full board of governors.

20. Key Links with other policies

This data protection policy is linked to our:

- Safeguarding (Child Protection) Policy and procedures.
- Safeguarding – Confidentiality and Information Sharing
- Online Safety Policy
- Data Breach Procedure
- Freedom of information publication scheme
- Acceptable Usage policies including Acceptable Use of ICT Agreements
- Photography, Filming and Use of images Policy
- Record Management policy
- Privacy notices
- Use of CCTV Policy
- School Mobile Telephone Use Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - lost;
 - stolen;
 - destroyed;
 - altered;
 - disclosed or made available where it should not have been;
 - made available to unauthorised people.
- The DPO will alert the Head, and the Chair of the Board of Governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - loss of control over their data;
 - discrimination;
 - identify theft or fraud;
 - financial loss;
 - unauthorised reversal of pseudonymisation(for example, key-coding);
 - damage to reputation;
 - loss of confidentiality;
 - any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school admin computer network, which is accessible by members of the admin team and the leadership team.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned;
 - the categories and approximate number of personal data records concerned;
 - the name and contact details of the DPO;
 - a description of the likely consequences of the personal data breach;
 - a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - the name and contact details of the DPO;
 - a description of the likely consequences of the personal data breach;
 - a description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

Our Lady's Abingdon is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - facts and cause;
 - effects;
 - action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored on the school admin computer network, which is accessible by members of the admin team and the leadership team. The DPO and Head will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Non-anonymised pupil exam results or staff pay information being shared with governors

- All paper documents recalled and shredded. If it is received by email, governors must only access using their encrypted email and they will be asked to delete the info.
- The governors confirm in writing that they have deleted the information.

A device containing non-encrypted sensitive personal data being stolen or hacked

- The incident will be reported to the police as soon as possible.
- If the device is a school registered device contact (the school IT supplier to wipe the device memory using appropriate software as soon as possible.
- If it is a personal device the member of staff must use their cloud supplier to wipe the device memory, they must confirm in writing that they have done this.
- Report to the DPO and assess what details could be accessible. The DPO will report to parents if suitable to the ICO

The school's cashless payment provider being hacked and parents' financial details stolen

- The school will immediately find out details of the breach.
- Parents will be notified immediately and asked to change their passwords if they consider they may be at risk.