



ALDENHAM
— FOUNDATION —

Data Protection Policy - Staff

**Reviewed January 2026
By the Bursar**

Key Staff Policy – Data Protection Policy

This new policy outlines your obligations to The Aldenham Foundation with regard to Data Protection.

Introduction

This Policy applies to all staff working in the Foundation (whether directly or indirectly), whether paid or unpaid whatever their position, role or responsibilities which includes employees, Governors, contractors, agency staff, work experience / placement students and volunteers. This Policy is about your obligations under the data protection legislation.

Data protection is about regulating the way the Foundation uses and stores information about identifiable people (Personal Data). It also gives people various rights regarding their data, such as the right to access the Personal Data the Foundation holds on them.

As a Foundation, we collect, store and process Personal Data about our staff, pupils, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in the Foundation and will ensure that we operate successfully.

You are obliged to comply with this Policy when processing Personal Data on our behalf. Any breach of this Policy may result in disciplinary action.

The Foundation has a number of documents relating to the handling of Personal Data. These are available within the Policies and Procedures area of SharePoint and on the School Portal.

The Bursar has been appointed the Data Protection Manager (DPM) for the Foundation and is responsible for helping you to comply with the Foundation's obligations. All queries concerning data protection matters should be raised with him.

Application

This Policy does not form part of your contract of employment and may be amended by the Foundation at any time.

Scope

Data protection concerns information about individuals.

Personal Data is data which relates to a living person who can be identified either from that data or from the data and other information that is available.

Information as simple as someone's name and address is their Personal Data.

So you can do your job, you need to use and create Personal Data. Virtually anything might include Personal Data.

Examples of places where Personal Data might be found are:

- On a computer database
- In a file, such as a pupil report
- A register or contract of employment
- Pupils' exercise books, coursework and mark books
- Health records
- Email correspondence

Examples of documents where Personal Data might be found are;

- A report about a safeguarding incident;
- A record about disciplinary action taken against a member of staff;
- Photographs of pupils;
- Contact details and other personal information held about pupils, parents and staff and their families;
- Contact details of a member of the public who is enquiring about placing their child at the Foundation;
- Financial records of a parent;
- Information on a pupil's performance; or
- An opinion about a parent or colleague in an email.

This list is not exhaustive, there may be many other processes that you use and create that would use Personal Data.

You must be particularly careful when dealing with Personal Data which falls into any of the categories below:

- Information concerning safeguarding matters.
- Information about confidential medical conditions and information about educational learning needs.
- Information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved).
- Financial information (for example about parents and staff).
- Information about an individual's racial or ethnic origin.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life.
- Genetic information.
- Information relating to actual or alleged criminal activity.
- Biometric information (e.g. an overseas pupil's biometric identity card).

These categories are referred to as Special Category Data in this Policy and in the Information Security Policy. If you have any questions about the processing of these categories of Personal Data please speak to the Bursar.

Your obligations

Personal Data must be processed fairly, lawfully and transparently. What does this mean in practice?

- "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.
- People must be told what data is collected about them, what it is used for and who it might be shared with, unless it is obvious. They must also be given other information such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (ICO - the data protection regulator). This information is provided in a document known as a Privacy Notice. Copies of the Foundation's Privacy Notices can be accessed on the Foundation's website. You must familiarise yourself with the Foundation's Privacy Notices.

If you are using Personal Data in a way you think an individual might think is unfair, please speak to the Bursar.

You must only process Personal Data for the following purposes:

- Ensuring that the Foundation provides a safe and secure environment.
- Providing pastoral care.
- Providing education and learning for our pupils.
- Providing additional activities for pupils and parents e.g. activity clubs.
- Protecting and promoting our interests and objectives e.g. fundraising.
- Safeguarding and promoting the welfare of our pupils.
- Fulfil our contractual and other legal obligations.

If you want to do something with Personal Data that is not on the above list, or is not set out in the relevant Privacy Notices, you must speak to the Bursar. This is to make sure we have a lawful reason for using the Personal Data.

We occasionally rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should speak to the Bursar if you think you may need to obtain consent.

You must only process Personal Data for limited purposes and in an appropriate way. *What does this mean in practice?* For example, if pupils are told they will be photographed to enable staff to only recognise them when writing references, you should not use those photographs for another purpose (e.g. in the Foundation's prospectus).

Personal Data held must be adequate and relevant for the purpose. *What does this mean in practice?* This means not making decisions based on incomplete data e.g. when writing reports you must make sure you are using all of the relevant information about the pupil.

You must not hold excessive or unnecessary Personal Data. *What does this mean in practice?* Personal Data must not be processed in a way that is excessive or unnecessary e.g. you should only collect information about a pupil's siblings if that Personal Data has some relevance.

The Personal Data that you hold must be accurate. *What does this mean in practice?* You must ensure that Personal Data is complete and kept up-to-date e.g. if a parent notifies you that their contact details have changed, you should ensure this is updated on iSAMS immediately.

You must not keep Personal Data longer than necessary. *What does this mean in practice?* The Foundation has a policy about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data. Please seek advice for guidance on the retention periods and secure deletion. You will also find our Data Retention and Erasure Policy on SharePoint.

You must keep Personal Data secure. You must comply with the following Foundation policies and guidance relating to the handling of Personal Data:

- Information Security Policy.
- Policy on the use of photographs and videos of pupils.
- IT Acceptable Use Policy for Staff.
- Data Retention Erasure Policy.

You must not transfer Personal Data outside the EEA without adequate protection. *What does this mean in practice?*

- We have safeguards in place for transfers outside of the EEA which relate to our routine activities. This would be relevant where, for example, we need to send pupil information to parents living overseas, or where you access your emails whilst on holiday outside of the EEA, or use cloud-based storage.
- However, if you need to transfer personal data outside the EEA for less routine reasons, please contact the Bursar. For example, if you are arranging a school trip to a country outside the EEA.

Sharing Personal Data outside the Foundation - dos and don'ts.

DO share Personal Data on a need to know basis - think about why it is necessary to share data outside of the Foundation - if in doubt, always ask your Head of Department or Manager.

DO make sure that you have permission from your Head of Department, Manager, Marketing Manager or the Bursar to share Personal Data on the Foundation's website.

DO be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from the Bursar where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from a parent but using a different email address).

DO be aware of "phishing". Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Do not reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT Department.

DO NOT disclose Personal Data to the Police without permission from either the Head of Foundation, Head of the Prep School or the Bursar (unless it is an emergency).

DO NOT disclose Personal Data to third parties, including volunteers or contractors without permission from the Bursar (unless there is a lawful reason to do so). This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event.

Sharing Personal Data within the Foundation

Personal Data must only be shared within the Foundation on a "need to know" basis.

Examples of sharing which are likely to comply with the Act include;

- A teacher discussing a pupil's academic progress with other members of staff e.g. to ask for advice on how best to support the pupil;
- Informing an exam invigilator that a particular pupil suffers from panic attacks; or
- Disclosing details of a Teaching Assistant's allergy to bee stings to colleagues so that you/they will know how to respond (but more private health matters must be kept confidential).

Examples of sharing which are unlikely to comply with the Act include;

- The Head of Foundation being given access to all records kept by Nurses working within the Foundation (seniority does not necessarily mean a right of access);
- Informing all staff that a pupil has been diagnosed with Dyslexia (rather than just informing those staff who need to know and teach the pupil); or
- Disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or it is an emergency).

You may share Personal Data to avoid harm, for example, safeguarding matters. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training please contact your school Designated Safeguarding Lead.

Individual's rights concerning their Personal Data.

People have various rights concerning their information.

You must be able to recognise when someone is exercising their rights (known as a Subject Access Request) so that you can refer the matter to the Bursar.

Please let the Bursar know immediately if anyone (either for themselves or on behalf of another person, such as their child);

- Wants to know what information we hold about them or their child;
- Asks to withdraw any consent that they have given to use their information or information about their child;
- Wants us to delete any information;
- Asks us to correct or change information e.g. bank details, health record (unless this is a routine update of information such as contact details);
- Asks for electronic information which they provided to us to be transferred back to them or to another organisation;
- Wants us to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as our newsletter or Old Aldenhamians (OA) events information; or
- Objects to how we are using their information or wants us to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

Requests for Personal Data (Subject Access Requests)

One of the most commonly exercised rights, mentioned above, is the right to make a Subject Access Request. Under this right, people are entitled to request a copy of the Personal Data which we hold about them (or in some cases their child) and to certain supplementary information.

Subject Access Requests do not have to be labelled as such and do not even have to mention data protection e.g. an email which simply states "Please send me copies of all emails you hold about me" is a valid Subject Access Request. You must always let the Bursar know immediately when you receive any such requests as we are required to act within a strict timeframe as set out by law.

Receiving a Subject Access Request is a very serious matter for us and will involve complex legal rights. Staff must never respond to a Subject Access Request themselves unless authorised to do so.

When a Subject Access Request is made, the Foundation must disclose all of that person's Personal Data to them which falls within the scope of his/her request. There are only very limited exceptions. There is no exemption for embarrassing information, so think carefully when writing letters and emails as they could be disclosed following a Subject Access Request.

However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding matters.

Breach of this Policy

Any breach of this Policy will be taken seriously and may result in disciplinary action.

A member of staff who deliberately or recklessly discloses Personal Data held by the Foundation without proper authority, is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.