ABBEY DLD
GROUP OF COLLEGES
CAMBRIDGE • LONDON • MANCHESTER

Data Protection FAQs

This document is intended to anticipate and answer questions you may have surrounding common questions about data protection, your personal data privacy rights and nature of data processing within the Abbey DLD Group.

What constitutes 'personal data'?
Personal data relates to a living individual who can be identified either from the data or from the data in conjunction with other information - for example a name plus a telephone number, address, date of birth, email address, photograph, and so on. Personal data also covers written comments about an individual e.g. a teacher's comment about a student in a professorial report and in general email correspondence.

What is Data Subject Access Request?
Right of Access, also known as a DSAR gives individuals the right to obtain a copy of their personal data being processed by a Controller as well as other supplementary information. This 'Right of Access' helps individuals to understand why and how you are using their personal data.

An organisation who has been issued with a DSAR has one calendar month from the date it is received to provide information to the individual. Where the controller requests identification from the individual then the date would start once the identification has been provided. For practical purposes, if a consistent number of days is required (e.g. for operational or system purposes), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.

A request can be made in writing or verbally and can be made to any part of an organisation (including via social media) and it does not have to be addressed to a specific person or contact point. A request does not have to include the phrase 'subject access request', as long as it is clear that the individual is asking for their own personal data.

What are the 7 UK GDPR data protection principles?
Data protection laws across the globe have always had at their heart core data protection principles. UK GDPR specifically stresses the requirement for organisations to be accountable. The seven principles are:
1. Lawfulness, Fairness & Transparency – ensure people are always aware of when and how their data is collected. Do not use personal data in a way that they would not reasonably expect.
2. Purpose Limitation – be clear about the purpose(s) you will use personal data for
3. Data Minimisation – only collect the personal data you need for your clear purpose(s)
4. Accuracy – personal data should not be inaccurate or misleading
5. Storage Limitation – don't keep personal data for longer than you need it for your clear purpose(s)
6. Security – ensure appropriate security measures are in place to protect personal data
7. Accountability – you must be able to demonstrate your commitment to all of the above.

What is a privacy notice and where should they be displayed?
A privacy notice is a public statement of how Abbey DLD Group applies data protection principles to processing data. It should be a clear and concise document that is accessible by individuals.
At every point where data collection happens there must be a privacy notice or statement. For example; when you send forms out to parents requesting information there must be a clear privacy statement or a link to the ADC privacy notice, which can be found on the ADC website.
We advise that for all forms you add the link to the group privacy notice.

Is it ok for students to sign up for extracurricular classes and other departmental activities via noticeboards?
Yes, this is fine as the student is selecting a class/activity and merely signing up. Once the list is no longer required it should be destroyed.

A student brings me a medical note after being absent from classes. Should I make a copy for myself and send one to the bursary?
No - there should only be one copy of this sensitive personal information and it should be held centrally on the student record.

We have a departmental mailing list where people have signed up to receive information about our activities. Can we still operate this?
Mailing lists can only operate with either the consent of the individuals on the list or under documented legitimate interest. UK GDPR also stipulates that individuals must be provided with a process, or instructions, whereby they can withdraw their consent from being included on a mailing list at any time, so you would need to make provision for this. Mailing lists that do operate should be stored within a system rather than in spreadsheets. This protects any updates to the process and centralised communications about changes that may affect the individual who has consented. If static files exist there is a risk that updates may be missed and we may not have the relevant evidence required by the ICO to say that we have the individuals' permission to use it. If we fail to update our records and subsequently contact an individual who has asked to be removed from our lists, this could result in a complaint.

Am I allowed to take documents on a USB home to work on them?
No, as this is a risk owing to the fact that a USB could be lost. If there is personal data on the USB, this would be a clear breach under UK GDPR.

All staff have access to Microsoft OneDrive, cloud storage for files from home via VPN, both of these options mean that taking a USB home to work is unnecessary. Contact the IT Department if you need any assistance with this.

One of the teachers in my department has asked me to log into their ADC email account to retrieve their monthly payslip. Am I allowed to do this?
No - this is a breach of the ADC IT policies and data protection. Staff should not share their log-in details with other colleagues and should be using their ADC email themselves.

My department uses contract staff for work. Do these people need to have ADC emails?
No, but they do need to exercise care and comply with data protection regulations in respect of personal data, as required by UK GDPR, in relation to their engagement with ADC.

Will we be allowed to take a copy of invoices from casual teachers or staff time sheets in case we need to chase payment with Finance?
It is ok to take a copy as long as it is not retained for longer than necessary (i.e. once the payment has been made). In practice though, ask yourself how often you actually need to chase payments (and specifically) provide a copy of the documentation again?

Do I need to delete emails that have personal information in them or in attachments (like student application forms)?

It is good practice under current Data Protection regulation to delete anything containing personal information unless there is a good operational reason to keep it for a specified period. Where you are keeping an attachment in an email for future reference it is good practice to save the document on a secure system and delete the email (see the ADC Retention schedule for more details).

What happens if I lose my personal notebook?
Personal notebooks strictly speaking wouldn't usually be covered by the UK GDPR. This being said sometimes you may collect sensitive or confidential information within your personal notes. If you feel this information would be damaging to an individual, if it was lost, then its always advisable to report the loss of them. It is also advisable to destroy notebooks once they are no longer required.

If the fee payer isn't the parent or guardian can I send them pupil information such as reports?
You can only share personal information when requested by a subject access request to the individual who has requested it. The only exemption being would either be to the parent of a child or an individual who has power of attorney. If the fee payer is neither a legal guardian nor has power of attorney this information can then only be shared with the consent of the data subject.

How do I know how long I need to keep data for?
Abbey DLD Group has a Retention Policy. This policy will detail how long all information should be kept for. If you are unsure or feel the policy misses something, then contact head office via dpo@abbeydld.co.uk .

I use social media for work, how does the UK GDPR affect me?
When using social media to share information (such as photos or videos) on data subjects, always make sure you gain consent of the individuals and can remove information upon request.

Can I keep using school photos after a pupil has left?
If you have gained and recorded consent, and it is clear that photos will be kept after a pupil has left then this is fine.

Can I use Whatsapp?
The use of any technology outside of the issued tools is not allowed and should not be used for official work purposes. Keep personal apps and tools for personal use only.

Can a parent or pupil request their data (SAR) verbally or do they have to go through the Abbey DLD process?
Individuals can request information in any way they see fit. This can be verbally, in writing or electronically. Abbey DLD have a process which we will always guide individuals to follow however data subject do not have to follow this process.

I'm a teacher – does the UK GDPR cover my job too?
Any individual who deals with peoples data is subject to the UK GDPR. Teachers will deal with a lot of pupil information and at times sensitive information. Therefore, all teaching staff need to be aware and trained on the legislation.

Can I share parents' details with other parents?
Yes, if the parents are aware of who their information will be shared with and that they have given consent for their information to be shared.

Can I use parents or students data to contact them for non-Abbey DLD business purposes?

No. This is unlawful under the UK GDPR & DPA 2018. Any employees using personal data inappropriately can be directly prosecuted and fined by the ICO.

What should I do if an organisation, such as the police or social services, requests information on one of our parents or students?
Care must always be taken to ensure that the sharing of personal data is done so lawfully and securely. In all cases, before you share data with any 3rd parties, you should contact the DPO (dpo@abbeydld.co.uk) to ensure the activity is allowed.

How can I check my current supplier contracts with to ensure they are UK GDPR compliant?
If you are unsure whether your contracts are UK GDPR compliant then contact head office on dpo@abbeydld.co.uk with the relevant information and we will review and recommend any necessary changes.

What process should I follow when bringing on a new supplier who will be handling our students or parents' data?
When looking to contract with a new supplier we have an obligation to ensure that they are UK GDPR compliant. They need to demonstrate this to us and contractual terms will also need to reflect the new Data Protection laws. When there is a change of a major supplier the business must also consider conducting a Data Privacy Impact Assessment (DPIA) to ensure the appropriate safeguards are in place. If you are unsure further guidance can be sought from the DPO (dpo@abbeydld.co.uk).

Can I take photos at events with parents for marketing and promotional purposes?
If you are running an event, inform attendees at the start and ask them if they are ok with photos being taken. Most event organisers give a visual key on a tabard of some sort to show those that don't want their pictures taken and delete those pictures where they are captured. Also, you can designate areas and times where photos are taken and make people aware so they can avoid those areas if needs be. If the event is in a public area then you have free reign to photograph whoever you want.

Secure destruction of paper based records
All paper records containing personal information should be destroyed securely. As a minimum they should be shredded. If the document contains confidential or sensitive information then measures should be taken to ensure the secure destruction of those documents.

Is there any basic guidance online that I can access?
Yes, the Information Commissioners Office (ICO) who has responsibility for enforcing UK GDPR in the UK has a range of guidance for organisations. This provides a useful overview of the basics in terms of what you need to do now: https://ico.org.uk/media/1624219/preparing-for-the-UK GDPR-12-steps.pdf

Can a parent can apply under a 'subject access request' to see anything written about a child (including references)?

Schools have an obligation to recognise such a request. Any data provided must have other names redacted, especially if it refers to staff or other pupils. If parents specifically ask to see a references, we tell them they can ask the recipient school for it (pointing out that it is best not to ask for this until they have heard from the school) and leave it up to them to share or not.

Do we need consent when seeking/providing student references?

There is an exemption in the DPA 2018 that allows the sending and receiving of confidential references for the purposes of educational references. This means that schools do not need to seek consent to send or receive references. However, it is advised that schools are transparent about this activity and include a statement in admissions policies, application forms and parental contracts as relevant.

Schools may wish to use/adapt this line:

In line with the Data Protection Act 2018, we may collect references from previous schools or education establishments as required by the application process. We may also send references to destination schools or educational establishments as part of the exit process.

If pupils personally ask within 12 months of leaving for a reference from us by means of written evidence of attendance, copies of lost reports or copies of exam certificates then as long as suitable ID is provided it is reasonable to provide this. Requests for this or any other information beyond 12 months after leaving date are best treated as a DSAR and recorded as such.

It is vital that any references we provide containing special category data, such as SEN or medical data, are sent securely using encryption or suitable postal arrangements.

Pupils will often at some point in their lives ask for a character reference from a member of staff, but these will be personal references and as long as this is made clear to the recipient they are not affected by the above rules.

Do we need to obtain permission from staff members for them to be included in public documents such as policies and student handbooks?

No, this forms part of staff's contractual obligations for their details to be used in policies and documents. We do however advise that you do make staff aware anytime when their details may be made public and searchable.

Can I use AI?

Yes. However, the AI platform you use and the information you input must be carefully considered. The Group's IT systems restrict access to unauthorised or inappropriate AI applications, helping to reduce the risk of data being shared with services that do not meet our security and data protection requirements.

For generative AI tools such as ChatGPT, Copilot and Claude, the Group's preferred platform is Microsoft Copilot. Copilot operates within Microsoft's enterprise environment, meaning that prompts and responses are protected by enterprise-grade security controls and are not used to train public AI models.

Nevertheless, all staff must exercise caution when using any AI tool. Personal data should be fully anonymised or removed wherever possible, and only the minimum amount of information necessary should be included in prompts. Staff remain responsible for ensuring that any use of AI complies with the Group's Data Protection, Confidentiality and Information Security policies.

Key principle: Never enter confidential, sensitive or personally identifiable information into an AI tool unless you are certain that the platform has been approved for that purpose and that appropriate safeguards are in place.