

The Data Protection Act – Guidance for staff

The Data Protection Act (DPA) is one of the three main pieces of legislation by which members of the public can request information from the School. The others are the Freedom of Information Act (FOI) and the Environmental Information Regulations (EIR), both covered in a separate guidance.

What the Act entails

The Data Protection Act concerns the safeguard of personal data. Its purpose is to balance the legitimate needs of organisations to collect and use personal data for business and other purposes, against the right of individuals for the privacy of their personal details. The legislation is underpinned by a set of eight straightforward, common-sense principles, which state that all personal data should be:

1. Fairly and lawfully processed
2. Processed for specified purpose(s)
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not kept longer than necessary
6. Processed in line with data subjects rights
7. Secure
8. Not transferred to countries without adequate protection

What constitutes Personal data.

Personal data can be any information which identifies a specific, living individual, whether it relates to personal or family life, business or profession. The ICO has published [a step by step guide](#) to what constitutes personal data, which you can access [here](#).

Examples of School information which would count as personal data are: staff and student files; email correspondence which describes or identifies an individual; references submitted to the School in support of promotion or employment, even if submitted in confidence, or as part of committee business.

Under the Data Protection Act, an individual is entitled to gain a copy of their personal data by making a Subject Access Request. There is a standard £10 charge for these requests, which must be made in writing and include proof of identification.

Dealing with a Subject Access request

We have a maximum of 40 days to respond to DPA requests. As soon as the request has been received, the Data Protection Officer will normally contact the areas involved and ask that they search their individual systems.

Under the DPA, a Data Controller (ie the School) is entitled to enter into negotiation with a data subject, to confirm the exact information he or she wishes to receive. During the period of negotiation, the Data Controller does not have to release requested information, if it is likely to prejudice those negotiations. Once the negotiations are complete, the Subject Access Request is dealt with in the normal way.

Please note: if a subject wishes to gain access to all their personal data held by the School, this is within their rights under the DPA.

Third party data

Any release of personal data must be checked to see whether it reveals the identity of a third party. This information can either be redacted, or the third party will be contacted to consent to the release of the information. If this proves to be difficult, Data Protection officer will need to balance

the rights of the third party against those of the data subject, to evaluate if it is reasonable to release the material.

Managing Personal Information

The Data Protection Act makes it necessary for us to manage personal information in the School fairly, securely and accurately. Consequently, it is important that you:

- Only collect the information you need for a particular job, and consider deleting or destroying it after that job is complete. Make sure any superfluous information is deleted or destroyed.
- File personal information properly, so that it is easy for you or a colleague to find it.
- Tell people why you are collecting their information, what it will be used for and who will see it. A statement to this effect is called the 'Privacy Notice.' For example, if you are collecting data for research and it is part of your funding agreement that the data, either fully or partially, will be passed to a data archive, it is essential that you inform the subject.
- Make sure the information is secure. Electronic information should be saved onto one of the School's secure network drives. If using portable storage media like memory sticks or hard drives like the C: drive, the information should be encrypted. You should also lock your computer when you are away from your desk and not allow other people to view computer screens showing personal information. Paper based information should be stored in lockable cabinets and not left out where other people can access it.
- Only release data to the subject of the information, or the staff who are qualified to use it. The School has to submit an annual list to the Information Commissioner's Office detailing what personal information we hold and who we will share it with, e.g. making student data available to HEFCE. There may be times when we are contacted by the Police or another state body requesting information about a student or staff member. In these cases, we will need written notice of the personal information they require.

If you have concerns or queries about Data Protection, please contact the Data Protection Officer for further guidance and advice.