# Guidance Note: Data Protection

Comprehensive information and guidance on the Data Protection Act 1998 can be found on the Information Commissioner's website at www.ico.gov.uk

References in this Guidance Note to schools/colleges includes academies.

**What is the purpose of the Data Protection Act 1998?**

Broadly speaking, The Data Protection Act 1998 ("DPA") was designed to do two things:-

1. To allow individuals access to information held about them;
2. To protect information about individuals being disclosed improperly.

The DPA provisions apply to the "processing of personal data" rather than applying to a particular category of persons or organisation.

"Processing" is defined as "obtaining, recording or holding the [data] or carrying out any operation or set of operations on the [data] including organising, amending, retrieving, using, disclosing, erasing or destroying [data]".

As can be seen, the scope of the DPA is wide enough that it applies to just about everything that may be done with an individual's personal details.

**How does the Data Protection Act 1998 apply to Schools/Colleges?**

Schools/Colleges will come into contact with information and/or data that is subject to the provisions of the DPA in their every day operation. As the employers of staff they will collect data relating to their staff for recruitment monitoring, contact databases etc. As institutions entrusted with the care of students they will collect data in compliance with other legislation such as that relating to pupil information, for example.

It is important for schools/colleges to understand the terminology used in the DPA so that they are better able to identify whether their actions fall within the scope of the legislation.

**What is covered by the Data Protection Act 1998?**

The DPA applies to the following matters and provides the following definitions:

- "Data" – information which is (or is intended to be) processed automatically or which does (or is intended to) form part of a Relevant Filing System or which forms part of an accessible record (e.g. health, education, housing, social services etc).

- "Relevant Filing System" – any set of information relating to individuals which is not processed automatically but which is structured by reference to individuals or to criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible.

  Note: If there is no structure to a system where personal and/or sensitive data is held which allows ready accessibility to relevant information it may not be considered a Relevant Filing System (although, generally speaking, filing systems by their very nature are structured).

- "Data Subject" – an individual who is the subject of Personal Data.

- "Data Controller" – the person who (either alone or jointly) determines the purposes for which, and the manner in which, Personal Data are, or are to be, processed. The Data Controller may be a company.

- "Data Processor" – any person who processes Personal Data on behalf of the Data Controller.

- "Processing" – obtaining, recording or holding the Data or carrying out any operation or set of operations on the Data including organising, amending, retrieving, using, disclosing, erasing or destroying Data.

- "Personal Data" – Data relating to a living individual who can be identified from that Data. (This does not include the mere mention of someone's name in a document (unless accompanied by other personal details about them)).

Personal Data in a school/college environment, particularly relating to the employment of staff, may include:

- Names, addresses, telephone numbers of employees, students and parents/carers
- Bank account details (for payroll, for example)
- Information about employees and students family members in cases where next of kin needs to be contacted
- Information about marital status (for insurance purposes)
- Information for the purposes of equal opportunities monitoring
- Personal details on job application forms

- "Sensitive Data" – Personal Data consisting of information on the Data Subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, or commission or proceedings for any offence committed by the Data Subject.

**Who Regulates compliance with the Data Protection Act 1998?**

The principles and purpose of the DPA are regulated by the Information Commissioner's Office ("the ICO"). The ICO has published a Code of Practice ("CoP")[1], under section 51 DPA, as part of its duty to promote good practice, entitled *'Subject Access Code of Practice – dealing with requests from individuals for personal information'*. The CoP gives advice on good practice although compliance with the recommendations is not mandatory where they go beyond the strict legal requirements of the DPA. The content of the CoP is, in the main, a consolidation of pre-existing guidance but with the addition of a few new issues for organisations to consider.

The ICO also issues guides specifically relating to data protection issues in schools, colleges and universities in the 'in your sector' section.

**What are the "best practice principles" of the Data Protection Act 1998?**

The 8 best practice principles are contained in Schedule 1 of the DPA and provide that:

1. Personal Data shall be processed fairly and lawfully.

   This covers the conditions required to have been satisfied so that "Personal Data" is considered to have been fairly processed. "Conditions" include necessity of contractual obligation, legal obligation, administration of justice, for a legitimate interest etc. It also stipulates the requirement that Data Subjects must give explicit consent for the processing of "Sensitive Data".

2. Personal Data shall be obtained only for one or more specified and lawful purposes.

3. Personal Data shall be adequate, relevant and not excessive in relation to the purpose for which it is being processed.

4. Personal Data shall be accurate and, where necessary, kept up to date.

5. Personal Data processed for any purpose shall not be kept for longer than is necessary.

[1] Updated Summer 2017.

6. Personal Data shall be processed in accordance with the Data Subject's rights under the DPA.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.

8. Personal Data shall not be transferred to countries outside the EEA unless there is an adequate level of protection.

The ICO gives detailed guidance on the application of these principles.

**Can an individual request information or data that a School/College holds about them?**

Yes. Every individual has the right to make a Subject Access Request ("SAR") to a Data Controller about Personal and/or Sensitive Data held about them and, if so, what it is, its source (if known), why it is being processed and to whom the data is or may be disclosed.

**What form does a SAR have to take?**

In order for a SAR to be valid:

- it should be made in writing
- it must relate to a living person (a request cannot be made on behalf of a dead employee/student).

The SAR need not expressly state that it is a request for information being made under the DPA. (Even where the incorrect legislation is quoted (e.g. Freedom of Information Act 2000 (if that does not apply)), the Data Controller must still comply with the request under the DPA). The individual making the SAR need not state the reason for making the request, neither are they required to disclose what they intend to do with the information once it has been provided.

**What if a SAR is made using social media – can it be a valid request?**

It is recognised that using, for example, a Facebook page or a Twitter account may not be the most effective way of delivering a SAR so that the organisation can identify it as being a SAR and process it accordingly, SAR's made in this way are perfectly valid (provided they meet the other eligibility criteria) and should be complied with. The CoP provides further information and guidance on SAR's made in this format, as well as further guidance on recognising SAR's.

**What duties must the Data Controller comply with before responding to a SAR?**

The Data Controller is under a duty to verify the Data Subject's identity where it receives a SAR. Obviously, if the request has come from an employee or student, verification of identity will not usually be an issue. However, if a SAR is made by a solicitor, for example, the Data Controller must first verify that the solicitor is authorised to make the SAR on behalf of the Data Subject (the solicitor should provide an original written, signed authority from the client). Failure to do so, and where the request for information is complied with (either in whole or in part), may result in the Data Controller being in breach of the DPA.

The Data Controller may request payment of a fee up to the value of £10.00. Traditionally the Data Controller has been able to delay responding to the SAR until such time that the payment is made, however, whilst it is still permissible to do so, this is likely to be revoked in the future and is, in any event, frowned upon by the ICO.

**How long does the Data Controller have to respond to a SAR?**

The Data Controller has up to 40 calendar days to comply with the SAR. This may be extended where, for example, extra time is needed to collate information being held by a third party e.g. outsourced HR or payroll. In all cases, it is prudent to respond to the SAR to acknowledge receipt of it and to provide the Data Subject with a time frame for dealing with the request which should ideally state whether it will exceed the 40 day limit.

**Can a School/College amend/delete the information?**

Once a SAR has been received a school/college must not amend or delete the recorded information.

**Is there any guidance to assist a School/College in responding to a SAR?**

The ICO issues detailed guidance from time to time and their website is very useful.

**Are there any limitations to the rights of a Data Subject to access information held about them?**

There are certain circumstances where a Data Subject is not entitled to access information being held about them and, where such information is requested, the Data Controller may lawfully refuse to comply with a SAR for such information. For example:

- Confidential References – a reference in respect of education, training and/or employment which is given in confidence by an employer to a third party is not required to be provided to the Data Subject where they make a SAR in respect of such reference. The Data Subject would need to make a SAR to the third

party who received the reference. This exception clearly only applies to references given and not to references received.

- Management Planning - Personal Data processed for the purpose of assisting the Data Controller in the conduct of any business or other activity is exempt from the SAR where to provide the information requested would prejudice the conduct of that business or other activity e.g. an employee cannot use a SAR to gain access to certain data if their employer is carrying out a redundancy exercise and disclosure of that information to the employee would prejudice the redundancy exercise.
- Legal Professional Privilege – information that is passed between the employer and their legal advisor for the dominant purpose of giving or receiving legal advice is exempt from being accessed by the Data Subject. Legal Professional Privilege exemption will not apply to legal advice/information which has been provided by the advisor to the employer and then shared by the employer with other staff members and/or third parties.

**What are the consequences of a failure to comply with the DPA 1998?**

A breach of the DPA may be a civil and/or criminal offence.

Civil Offences:

Failure to properly comply with a SAR may result in the Data Subject making a statutory request to the ICO to determine whether or not the SAR has been carried out lawfully. The ICO can serve an Information Notice or Enforcement Notice on the organisation requiring them to provide the information so requested. (Data Controllers should note that a failure to comply with an Information or Enforcement Notice is a criminal offence).

A Data Subject may also issue court proceedings requesting an Order for compliance and/or make a claim for damages if they can show that they have suffered loss, or a claim for compensation for distress caused.

Criminal Offences:

Most of the offences created by the DPA are “triable either way” which means that the case will be heard in either the Magistrates or Crown Court depending on the facts of the case and whether the offence exceeds the Magistrate’s sentencing powers.

Some of the offences under the DPA which attract criminal liability include:

- Unlawfully obtaining, disclosing or procuring the disclosure of Personal Data;
- Selling, or offering to sell, Personal Data which has been unlawfully obtained;
- Processing Personal Data without notifying the ICO (if notification is required);

- Failure to comply with an Information or Enforcement Notice or an information notice, or knowingly or recklessly making a false statement in compliance with an Information Notice.

Further, the DPA refers throughout to "lawfulness". Generally speaking this indicates that a failure to comply with a requirement to do something "lawfully" may attract civil or criminal liability. Where it can be shown that processing of Personal Data is not lawful, it follows that unlawful processing is a criminal offence. This means that it is a criminal offence under the DPA to process Personal Data where there is, or could be:

- A breach of a duty of confidence;
- An infringement of copyright;
- A breach of an enforceable contractual agreement;
- A breach of the Human Rights Act 1998.

So, to provide a very real scenario, it will be a breach of the DPA if, in validly complying with a SAR, the Data Controller provides Personal Data relating to another which is capable of identifying that other. In many cases it will be necessary for the Data Controller to provide information in a redacted format so that any personal details that do not relate to the Data Subject are not inadvertently disclosed and so breach the organisation's DPA obligations to other persons. This may mean, for example, redacting a telephone directory which lists all staff members' contact details so that only the Data Subject's details remain. Of course, there will be situations where redacting a document will not sufficiently protect the identity of another individual who is not the Data Subject. In such a case, the Data Controller must weigh up the obligations placed upon them to comply with the Data Subject's SAR as against its duty to ensure that it does not breach any other DPA requirements.

**What is the General Data Protection Regulation?**

The General Data Protection Regulation (GDPR) 2016 came into force on 24th May 2016 and will apply in all Member States of the European Union from 25th May 2018. It will replace the Data Protection Act 1998.

The GDPR is built on the same fundamental principles as the DPA but there are distinct changes as a result of developments in technology and working environments. It will have a major impact on the way organisations manage personal data such as web privacy and employee records.

Schools and academies and other organisations in diocesan control are very likely to be recognised as UK data controllers and will, therefore, need to have a practical understanding of the implications and legal requirements of the GDPR in readiness for 25th May 2018. The CES therefore strongly recommends that specialist advice is sought to ensure compliance.

The effect of Brexit

UK data controllers may have delayed making preparations to comply with the GDPR due to the uncertainty of the future of the relationship between the UK and Europe. However, action must be taken to comply with the GDPR as it very likely to apply (even for a short period of time) because:

1. The government has now confirmed that the UK will implement the GDPR as the UK will still be a member of the EU in 2018. Article 50 was invoked in March 2017 so the exit date is now likely to be in March 2019 meaning that UK data controllers will have been subject to the GDPR for nearly a year.

2. When we do leave the EU the UK will want to ensure that UK businesses can continue to process EU data, a simple method of doing so would be to subscribe to the terms of the GDPR even if the UK is no longer a Member State and so bound by it.

Although this is not a comprehensive list of all the changes, some of the issues that UK data controllers will need to look out for include:

1. **Enforcement -** The maximum penalty for failure to comply has significantly increased from a £500,000 fine to the greater of 4% of an organisation's annual worldwide turnover or €20 million.

2. **Consent** - Employers will no longer be able to rely on implied consent when processing personal data. Consent will need to be given by clear affirmative action. Consent is presumed not to be freely given if there is a clear imbalance between the parties, particularly between an employer and employee. Therefore, employment contracts cannot be made conditional upon consent to processing or use of data.

3. **Data Subject Access Requests (DSAR)**: Employers must reply within one month from the date of receipt of a request rather than the current 40 days. The £10 fee is also being abolished unless a request is 'manifestly unfounded or excessive'. There is an emphasis on transparency which requires employers responding to a DSAR to explain how they approached it.

4. **Expanded territorial scope**: Non-EU data controllers and processors will have to comply if they offer goods or services to data subjects in the EU or monitor data subjects' behaviour within the EU (for example if a school in the UK liaises with schools outside of the EU (or post Brexit within the EU) where data is being held on EU citizens).

5. **Breach**: Employers must notify the regulator of all data breaches without delay and, where feasible, within 72 hours unless it is unlikely to result in risk to individuals. If a data breach involves a high risk to individuals then the employer must inform subjects without undue delay.

6. **Privacy by design:** This means building privacy into the design of your systems as the default setting, ensuring personal data is kept secure and destroyed when it is no longer needed, providing users with transparency and meaningful choice with respect to the use of their data, and avoiding unnecessary trade-offs between privacy and other interests

7. **Right to be forgotten:** Individuals have the right to have personal data erased where: the data is no longer necessary for the purposes for which it was collected; they withdraw consent and the data controller has no other legal basis to use the data; they object and there is no overriding legitimate basis for the processing; and the data have been unlawfully processed.

**What you should do now?**

UK data controllers, which will almost certainly include schools and academies, should start their preparations now in order to comply by 25th May 2018 given the amount of personal data and, in particular, sensitive personal data processed in relation to employees and pupils. They should:

- ✓ Carry out an assessment (and seek specialist advice if required):

  - Find and identify the data held
  - Understand the differences between the Data Protection Act 1998 and the GDPR
  - Ensure there are policies to demonstrate compliance with the GDPR
  - Carry out Data Protection Impact Assessments: assess existing compliance strategies and programmes
  - Decide how consent should be obtained: a standard provision in an employment contract to obtain consent to process personal data is likely to be ineffective under the GDPR. Employers should consider a separate declaration

- ✓ Follow ICO's recommendations including:

  - Creating awareness among senior decision-makers
  - Auditing and documenting the personal data held and
  - Recording where it came from and
  - Who it is shared with and
  - Reviewing the legal basis for the data processes carried out

- ✓ Develop and implement a data breach response plan and consider how to bring into effect the right to erase personal data.

- ✓ With large volumes of data, consider how to respond to DSARs within the new time frame.

- ✓ Make a decision on what is required for compliance in good time before 25th May 2018.

- ✓ Assess and make provision for the costs for compliance in your next financial budget.

The CES has briefed all Diocesan Education Services on the GDPR and, therefore, Catholic schools and academies should contact their own Diocesan Education Service for further information in the first instance. Once again, we would reiterate our recommendation that schools and academies seek specialist advice to ensure compliance with the GDPR.