

Leicester City Council

Data Protection Policy for Schools



Schools Data Protection Policy
2016 v1.0

Document: Data Protection Act Policy for Schools

Responsibility: It is the responsibility of the Governors to ensure procedures are in place to ensure that the school complies with the Data Protection Act 1998 (DPA)

Contents:

1. Introduction
2. Scope
3. Responsibilities
4. The Requirements
5. Notification
6. Privacy Notices
7. Conditions for Processing
- 8.
9. 8. Provision of Data
- 10.9. The individual's right to access their personal information (Subject Access Requests)
- 11.10. Provision of data to children
- 12.11. Parents' rights
- 13.12. Information Security
- 14.13. Maintenance of up to date data
- 15.14. Inaccurate Data
- 16.15. Recording of Data
- 17.16. Photographs
- 18.17. Breach of the policy
19. Further Information
20. Review of the policy
- 21.20. Abbreviations
- 22.21 Glossary

1. Introduction

In order to operate efficiently Ellesmere College has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

The School is committed to ensuring personal information is properly managed and that it ensures compliance with the Data Protection Act 1998 (DPA). The School will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

2. Scope

This policy applies to all employees, governors, contractors, agents and representatives and temporary staff working for or on behalf of the School.

This policy applies to all personal information created or held by the School in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, email, filing cabinet, shelving and personal filing drawers).

The DPA does not apply to access to information about deceased individuals.

3. Responsibilities

Overall responsibility for ensuring that the School meets the statutory requirements of the FoIA, EIR and DPA lies with the Governors and the Chair of Governors has overall responsibility for information management issues. They have delegated the day-to-day responsibility of implementation to the Head teacher.

The Headteacher is responsible for ensuring compliance with the DPA and this policy within the day to day activities of the School. The Headteacher is responsible for ensuring that appropriate training is provided for all staff.

All members of staff or contractors who hold or collect personal data on behalf of The School are responsible for their own compliance with the DPA and must ensure that personal information is kept and processed in-line with the DPA.

4. The Requirements

The DPA stipulates that anyone processing personal data must comply with eight principles of good practice; these principles are legally enforceable. The principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;

3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual, but need not be sensitive information. It can be as little as a name and address. Such data can be part of a computer record or manual record.

5. Notification

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the School is registered.

The School will review the Data Protection Register (<https://ico.org.uk/esdwebpages/search>) annually, prior to renewing its notification to the Information Commissioner.

6. Privacy Notices

Whenever information is collected about individuals they must be made aware of the following:

- The identity of the data controller, e.g. the School;
- The purpose that the information is being collected for;
- Any other purposes that it may be used for;
- Who the information will or may be shared with; and
- How to contact the data controller.

This must be at the time that information first starts to be gathered on an individual. The School will issue a Privacy Notice annually to all pupils and parents. This can be found on Leicester City Council's website under 'Privacy notice for pupils in school.'

7. Conditions for Processing

Processing of personal information may only be carried out where one of the conditions of Schedule 2 of the DPA has been satisfied.

Processing of sensitive personal data may only be carried out if a condition in Schedule 3 is met as well as one in Schedule 2.

8. Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- Other members of staff on a need to know basis;
- Relevant Parents/Guardians;
- Other authorities if it is necessary in the public interest, e.g. prevention of crime, safeguarding;
- Other authorities, such as the Local Authority and schools to which a pupil may move, where there are legitimate requirements (DfEE leaflet 0015/2000 entitled "Pupil Records and Reports" issued in March 2000 covers Data Protection issues and how and what information should be transferred to other schools. DfES/0268/2002 provides further information).

The School should not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Where there is doubt, or statutory requirements conflict, legal advice should be obtained.

When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled. Care must always be taken when there is any doubt about parental responsibility.

9. The individual's right to access their personal information (Subject Access Requests)

Any person whose details are held by the School is entitled, under the DPA, to ask for a copy of information held about them (or child for which they are responsible). They are entitled to see if the data held are accurate, and who it is shared with.

When a request is received it must be dealt with promptly; a response must be provided as soon as possible and within 40 calendar days and in some instances, for education records, 15 school days.

The School may make a charge of up to £10 for responding to a subject access request and up to £50 (on a sliding scale for photocopying charges) for access to a pupil's educational record.

When providing the information the School must also provide a description of why the information is processed, details of anyone it may be disclosed to and the source of the data.

10. Provision of data to children

In relation to the capacity of a child to make a subject access request, guidance provided by the Information Commissioner's Office has been that by the age of 12 a child can be expected to have sufficient maturity to understand the nature of the request. A child may of course reach sufficient maturity earlier; each child should be judged on a case by case basis.

If the child does not understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child and receive a response.

Pupils who submit requests to access their educational records should be allowed to do so unless it is obvious that they do not understand what they are asking for.

11. Parents' rights

An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the School is entitled to request relevant documentation to evidence this as well as the identity of the requestor and child. The School has the right to ask the Child if they object to release of information to the Parent if the Child is deemed mature enough to make such a decision.

In addition, parents have their own independent right under The Education (Pupil Information) (England) Regulations 2000 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records (as defined in the Education Act).

12. Information Security

All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. For example, possibilities may arise when computer screens are visible to the general public; files may be seen by the cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).

The use of computer passwords is a requirement of the school to avoid unauthorised access. All removable devices e.g. laptops, USB sticks. Personal mobile phones and digital cameras must not be used to store School data unless they comply with a School Bring Your Own Device (BYOD) policy, and should be encrypted and passworded wherever possible.

13. Maintenance of up to date data

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes. In reality most

relevant information should be kept for the period during which the person is associated with the School plus an additional period which the School has determined. The School may produce a Retention and Disposal Policy to clarify this.

14. Inaccurate Data

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. This is a section 10 request and must be answered within 21 calendar days by law. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

15. Recording of Data

Records should be kept in such a way that the individual concerned can inspect them. It should also be borne in mind that at some time in the future the data may be inspected by the courts or some legal official. It should therefore be correct, unbiased, unambiguous, factual and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Any person whose details, or child's details, are to be included on the School's website will be required to give written consent. At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

16. Photographs

Whether or not a photograph comes under the DPA is a matter of interpretation and quality of the photograph. However, the School takes the matter extremely seriously and seeks to obtain parents' permission for the use of photographs outside the School and, in particular, to record their wishes if they do not want photographs to be taken of their children.

17. Breach of the policy

Non-compliance with the requirements of the DPA by the members of staff could lead to serious action being taken by third parties against the school authorities. Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal. It should be noted that an individual can commit a criminal offence under the Act, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the data controller.

18. Further Information

Further advice and information about the DPA, including full details of exemptions, is available from the ICO website at www.ico.org.uk, or from Leicester City Council's Information Governance & Risk Team.

19. Review of the Policy

This policy is to be reviewed bi-annually.

20. Abbreviations

| Abbreviation | Description |
|--------------|--|
| DPA | Data Protection Act 1998 |
| EIR | Environmental Information Regulations 2004 |
| FoIA | Freedom of Information Act 2000 |

21 Glossary

| | |
|--------------------------|--|
| Data Controller | A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files. |
| Data Subject | The individual who the data or information is about |
| Educational record | The educational record is confined to information that comes from a teacher or other employee of a local authority or school, the pupil or their parents. Communications about a particular child from head teachers and teachers at a school and other employees at an education authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the governing body under a contract of services. It may also include information from the child and their parents, such as information about the health of the child. Information kept by a teacher solely for their own use does not form part of the official educational record. |
| Information Commissioner | The independent person who has responsibility to see that the DPA is complied with. They can give advice on data protection issues and can enforce measures against individuals or organisations who do not comply with the DPA. |
| Notified Purposes | The purposes for which the school is entitled to process that data under its notification with the Office of the Information Commissioner. |
| Personal Data | Defined in s(1) of the DPA, as 'data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller' (the school is a data controller), and includes any expression of opinion about the individual and any indication |

| | |
|-------------------------------|--|
| | of the intentions of the data controller or any other in respect of the individual. |
| Processing | covers a broad range of activities such that virtually any use of personal information or data will amount to processing. |
| Processed fairly and lawfully | Data must be processed in accordance with the 3 provisions of the DPA. These are the data protection principles, the rights of the individual and notification. |
| Sensitive Data | Information about racial or ethnic origin, sexual life, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence. |
| Subject Access Request | An individual's request for personal data under the Data Protection Act 1998. |