



Derbyshire Education Authority

Data Protection Policy for Schools

Information
and
Guidelines

Contents

This pack contains various guidelines and samples to help schools to create a policy for the way in which personal information relating to pupils and employees, is held and handled by the school, both paper and electronic records, and with particular reference to the requirements of the Data Protection Act 1998.

Each school should have a cabinet file for Data Protection matters and it should contain the following items:

- The school's Data Protection Policy document
- The school's current Registration documents
- The disclosures log
- Any guidelines or notices issued by the Information Commissioner or the Education Authority
- And subject access forms or data collection forms

If you require help or advice please contact

**The Education ICT Service
County Hall, Matlock DE4 3AG**

(Phil Land)

phil.land@education.derbyshire.gov.uk

**Tim Turner, Data Protection Officer
Corporate Resources Department
County Hall, Matlock DE4 3AG**

tim.turner@derbyshire.gov.uk

Bennerley Fields School Data Protection Policy

General Statement

The Headteacher and Governors of the school intend to comply fully with the requirements and principles of the Data Protection Act 1998.

All staff involved with the collection, processing and disclosure of personal data will be aware, and at appropriate times, be reminded of their duties and responsibilities within these guidelines.

Enquiries about the policy, the Notification and the data held on the computer(s)

Information about the Data Protection policy is available from the Headteacher and/or the School Business Manager and general information about the Data Protection Act can be obtained from the Education ICT Service, County Hall, Matlock..

Fair Obtaining

The School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data is held, the likely recipients of the data and the data subjects right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally the person collecting the data will explain the issues before obtaining the information.

Registered Purposes

The Data Protection Notification entries for the school are available for inspection at the school office

Explanation of any codes and categories entered is available from the School Business Manager.

Registered purposes covering the data held at the school are listed on the school's Notification and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

Data Integrity

The school undertakes to ensure data integrity by the following methods:

Data Accuracy – data held will be as accurate and up to date as is reasonable possible. If a data subject informs the school of a change of circumstances their records will be updated as soon as practicable.

Where a data subject challenges the accuracy of their data, The school will consult the local authority and follow approved procedures to consider the validity of the data.

Data Relevance – data held about people will be relevant to the purpose for holding the data. We shall not hold any data which are excessive in relation to the purpose. In order to ensure compliance with this principle the school will monitor data filed to ensure only what is required is filed (Headteacher and school clerk) and will respond to requests by parents or outside agencies in considering deletion of data.

Length of Time – data held about individuals will not be kept for longer than is necessary for the purposes registered. It is the duty of the school Headteacher and/or School Business Manager) to ensure that any obsolete data are erased.

Subject Access

The Data Protection Act extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that access should be granted as soon as this can practically be arranged, with the subject being invited at a Mutually convenient time, to view the file. Should parents require a copy of data filed there is likely to be a cost which will cover this.

Students/parents should ask for the data access form.
Available from the School Administrator
and staff should also use the relevant form
available from the School Administrator

Completed forms should be submitted to the School Administrator

Authorised Disclosures

The School will only disclose data about individuals, in general, with their consent. However there are any circumstances under which the school's authorised officer(s) may wish to reveal data without express consent. These circumstances are limited to emergencies such as information needed by the school nurse and/or the local health authority, emergency disclosures, statistical data in relation to education and legal requirements.

Data and Computer Security

The School undertakes to ensure security of personal data by the following methods :

Physical Security including: locked office door, window grills, locked filing cabinet.

Logical Security password protected computer systems, computers physically secure (also as above).

Procedural Security – applications for computer access, shredding of confidential waste, security of printouts etc.

Overall security policy is determined by the headteacher and governors and will be monitored and reviewed as appropriate and whenever a major security breach or loophole is apparent. The School's security policy is kept in a safe place at all times.

Any queries or concerns about security of data within the school should be brought to the attention of the headteacher.

Individual members of staff can be liable in law under the terms of this Act. They may also be subject to damages claims from persons harmed as a result of inaccuracy, unauthorised use or disclosure of their data. Any deliberate breach of this Data Protection Policy will be treated as a disciplinary matter and serious breaches may lead to dismissal.

Further details can be obtained from

A Harrison, Headteacher, Bennerley Fields School,
Stratford Street, Ilkeston, Derbyshire.

Bennerley Fields School

Data Protection Policy

General Statement

The Headteacher and Governors of this School intend to comply fully with the requirements and principles of the Data Protection Act 1998. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities within these guidelines.

Enquiries

Information about the School's Data Protection policy is available from the headteacher and general information about the Data Protection Act can be obtained from the Derbyshire Education Department's Data Protection Liaison Officer at County Hall.

Fair Obtaining

The School undertakes to obtain and process personal data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' rights of access. Information about the use of personal data is printed on the appropriate collection form, if details are given verbally the person collecting will explain the issues before obtaining the information.

Registered Purposes

The Data Protection Registration entries for the School are available, by appointment, for inspection in the school office. Explanation of the codes and categories entered is available from the headteacher.

Who is the person nominated to deal with Data Protection issues in the school. Registered purposes covering the data held at the school are listed on the school's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subjects' consent.

Data Integrity

The School undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their record will be updated as soon as is practicable. Where a data subject

Continued

challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate (challenged). We shall try to resolve the issue informally but if this is not possible, any disputes will be referred to the Board of Governors for their deliberation.

If the problem is not resolved at this stage independent arbitration may be sought by either side. Until resolved, the challenged marker will remain and all disclosures of the affected information will contain both versions of the information. In order to prevent such problem areas we shall provide data subjects with opportunities to check their data accuracy and request amendments.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive to the purpose for holding the data. In order to ensure compliance with this principle, the School Clerk will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the School Clerk, with appropriate guidance, to ensure obsolete data are properly erased.

Subject Access

The Data Protection Act extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received in respect of a pupil, the school's policy is that :

- Requests from parents of their own child will, provided that the child does not understand the nature of subject access requests, be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.
- Requests from pupils who do NOT understand the nature of the request will be referred to the child's parents
- Requests from pupils who can demonstrate an understanding of the nature of their request will be processed as any subject access request as outlined below and the copy will be given directly to the pupil.

Continued

Processing Subject Access Requests

Students/parents should ask for the [Subject Access](#) form available from the School Office and staff should use the [Staff Request](#) form available from the Headteacher. Completed forms should be submitted to the headteacher. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, indicating the date of receipt, data subject's name, name and address of requester (if different), type of data required (e.g. Student Record, Personnel Record) and planned date of supplying the information (not more than 40 days from the request date).

Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

Authorised Disclosures

In general, the School will only disclose data about individuals with their consent. However, there are circumstances under which the school's authorised officer(s) may wish to reveal data without express consent.

These circumstances are intentionally limited to :

- Pupil data disclosed to authorised recipients in respect of education and administration necessary for the school to perform its legitimate duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their children's health, safety and welfare
- Pupil data disclosed to parents in respect of their children's progress, attendance, attitude and general demeanour within, and in the vicinity of, the school
- Staff data disclosed to the relevant authority in respect of payroll and schools' staff administration
- Other disclosures as may prove unavoidable, for example where an incidental disclosure occurs when an engineer is fixing the computer systems. In such cases, the engineer will sign a document to promise NOT to disclose such data outside the school. Education Authority IT Liaison/Support Officers are professionally bound not to disclose such data.

Only authorised and properly instructed staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare workers must be made available only if the staff member **needs to know** the information for their work within the school.

Continued

Data and Computer Security

The School undertakes to ensure security of personal data by the following general methods – (for security reasons we cannot reveal precise details in this document) :

Physical Security

Appropriate building security measures are in place, such as alarms, window bars, lockable cabinets, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes, printouts and files are locked away securely when not in use. Visitors to the school are required to sign in and out and are, where appropriate, accompanied.

Logical Security

Security software is installed on all computers containing personal data, only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly. Filing cabinets should be kept locked when the room is unattended.

Procedural Security

In order to be given authorised access to the computer, staff will be properly checked and will sign a confidentiality agreement. All staff are trained and instructed in their Data Protection obligations and their knowledge updated as necessary. Computer printout and source documents are always shredded before disposal.

Overall security policy is determined by the headteacher and governors and will be monitored and reviewed as appropriate and whenever a major security breach or loophole is apparent. The School's security policy is kept in a safe place at all times. Any queries or concerns about security of data within the school should be brought to the attention of the headteacher.

Individual members of staff can be liable in law under the terms of this Act. They may also be subject to damages claims from persons harmed as a result of inaccuracy, unauthorised use or disclosure of their data. Any deliberate breach of this Data Protection policy will be treated as a disciplinary matter and serious breaches of the Act may lead to dismissal.

Further details on any aspect of this policy and its implementation can be obtained from the school.