



Aldercar High School

In pursuit of excellence

Daltons Close, Langley Mill, Nottingham NG16 4HL
Tel: (01773) 712477 Fax: (01773) 531969
E-mail: info@aldercar.derbyshire.sch.uk
www.aldercarhighschool.co.uk

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 of the school's duties and responsibilities under the Data Protection Act 1998. Staff will be given training on the requirements of the Act as and when it is considered appropriate.

Enquiries

Information about the School's Data Protection policy is available from the School Business Manager. The policy is made available to all staff on the IT network. The general public can view the policy on the school website [www.aldercarhighschool.co.uk] and general information about the Data Protection Act can be obtained from the Derbyshire Children and Younger Adults Department Data Protection and Freedom of Information Officer at County Hall : 01629 536470.

Fair Obtaining

The School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for the collection of the data, the purposes for which the data is held, the likely recipients of the data and their right to access that data either under the Education (Pupil Information) (England) Regulations 2005 or the Data Protection Act 1998. Data subjects will be informed about the collection and use of their data through the use of Privacy Notices which will be printed on the appropriate collection forms. There is a general Privacy Notice which can be found on the school's website at www.aldercarhighschool.co.uk. If these details are given verbally to the data subject the person collecting the data will explain the issues before obtaining the information.

Registered Purposes

The school's Notification with the Information Commissioner is available, by appointment, for inspection in the school office. Explanation of the codes and categories entered is available from the School Business Manager. Information held for the purposes stated on the school's notification document 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 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 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 which the data is held. In order to ensure compliance with this principle, the Personnel Manager/Data Manager 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

Personnel Manager – staff,
Data Manager – student data
SENCO – medical and SEN student data
Head of Post-16 – Post 16 student data
Child Protection Co-ordinator – safeguarding/child protection data

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 about the data held about their own child will, provided that the child is not of an age or ability to understand the nature of a subject access request, 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.

Processing Subject Access Requests

Students/parents should ask for the [Subject Access](#) form available from the Data Manager and staff should use the [Staff Request](#) form available from the Personnel Manager. Completed forms should be submitted to the Data Manager [students] / Personnel Manager [staff].

Provided that there is sufficient information to process the request, a response will be made and the Subject Access Form will be held on file with the date of 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 response 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 it is necessary for the school's authorised officer(s) to disclose data the without express consent of the data subject.

These circumstances are 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 a pupil's health, safety and welfare.
- Data contained within a Pupil's educational record will be disclosed to the child's parents if requested in accordance with Educational (Pupil Information) (England) Regulations 2005.
- Staff data disclosed to the relevant authority in respect of payroll and school's 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 undertake

NOT to disclose such data outside the school. Local Authority IT Liaison/Support Officers are professionally bound not to disclose such data.

Only authorised and properly instructed staff are permitted 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.

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, lockable cabinets, lockdown of computers if unattended for 10 minutes. Only authorised persons are allowed in key areas of the school including

- Main Office,
- Business Manager's Office
- Personnel Manager's office
- Data Office
- IT Technical staff office.

Portable storage devices, 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 given induction by the ICT Systems & Network Manager. All staff are trained and instructed in their Data Protection obligations and their knowledge updated as necessary. Computer printout and source documents are always disposed of securely.

Overall security is determined by the school governors and will be monitored and reviewed as appropriate and whenever a major security breach or loophole is apparent. Any queries or concerns about security of data within the school should be brought to the attention of the Headteacher. 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.

SUBJECT ACCESS FORM - STAFF

DATE OF REQUEST.....

NAME OF STAFF MEMBER [data subject].....

NAME OF REQUESTER.....

ADDRESS OF REQUESTER.....

TELEPHONE CONTACT DETAILS.....

RELATIONSHIP OF REQUESTER TO STAFF MEMBER.....

REASON FOR REQUEST.....

DATA REQUIRED.....

For office use

REQUEST APPROVED YES NO

IF NO, GIVE REASON.....

FURTHER INFORMATION REQUIRED: YES NO

IF YES, GIVE DETAILS:.....

DATE OF RESPONSE.....

NAME OF RESPONDING OFFICER

POSITION.....

SIGNATURE OF OFFICER.....

SUBJECT ACCESS FORM – STUDENT

DATE OF REQUEST.....

NAME OF STUDENT [data subject].....

NAME OF REQUESTER.....

ADDRESS OF REQUESTER.....

.....

TELEPHONE CONTACT DETAILS.....

RELATIONSHIP OF REQUESTER TO STUDENT.....

.....

REASON FOR REQUEST.....

.....

DATA REQUIRED.....

.....

.....

For office use

REQUEST APPROVED YES NO

IF NO, GIVE REASON.....

.....

.....

FURTHER INFORMATION REQUIRED: YES NO

IF YES, GIVE DETAILS:.....

.....

DATE OF RESPONSE.....

NAME OF RESPONDING OFFICER

POSITION.....

SIGNATURE OF OFFICER.....