



DATA PROTECTION POLICY

Data Protection Act 1998

1. Introduction

The Data Protection Act 1998 came into force on 1st March 2000 after receiving Royal Assent on 16th July 1998.

The Act repeals the Data Protection Act 1984 and certain other legislation that gives us rights of access to information held by organisations, including the Access to Personal Files Act 1987.

The Act extends the rights given to individuals in previous legislation and requires data controllers (people or organisations that hold and process details of living individuals) to comply with the Eight Principles (rules governing the use of personal data) and to bear in mind the rights and freedoms of those individuals when processing their details.

This document explains how The School will meet the legal requirements of the Data Protection Act 1998.

2. Statement of Intent

The School intends to fulfil all its obligations under the Data Protection Act 1998.

The School will ensure that the Information Commissioner is notified of all registrable processing and will conduct a periodic review and update of the register entries to ensure that they remain up to date.

It is the aim of The School that all appropriate staff are properly trained, fully informed of their obligations under the Data Protection Act 1998 and are aware of their personal liabilities.

Any employee deliberately acting outside their recognised authority will be subject to The School's disciplinary procedures, up to and including dismissal where appropriate, and, to possible legal action.

Individuals whose information is held and processed by The School can be assured that The School will treat their personal data with all due care.

It is possible that other legislation may (at times and under certain conditions) override Data Protection law - individuals should note that The School intends to fulfil all of its legal responsibilities.

This policy document applies only to information covered by the Data Protection Act 1998 and will be updated/amended as necessary according to the laws of England and Wales.

3. Fair Obtaining/Processing

The School will, as far as is practicable, ensure that all individuals whose details it holds are aware of the way in which that information will be held, used and disclosed.

Processing within The School will be fair and lawful, individuals will not be misled as to the uses to which The School will put the information given. It is perfectly acceptable for any person to ask the reason why the School is collecting data about them and what it will be used for.

If a person feels they have been deceived or misled as to the reason for which their information was collected, they should use the complaint procedure as detailed at the end of this document.

People are free to ask the person collecting the information why they want the details and what they will be used for.

If asked, staff should use the following 'fair obtaining' statement:

"Data Protection Legislation

The information you have provided will only be held for the purposes of processing and administration and will not be passed to any other organisation or third party."

Any individual whose personal data (including photographs) are to be included in the School's web site will be asked to give explicit consent.

At the time of data collection, it will be made clear to individuals that details published on the School's web site are viewable by anyone, anywhere in the world, who has access to the Internet.

4. Data Uses and Processes

The School will not use or process personal information in any way that contravenes its notified purposes or in any way that would constitute a breach of Data Protection law.

Any new purposes introduced will, where appropriate, be notified to the individual and - if required by the law - their consent will be sought.

The notification document can also be viewed on the Information Commissioner's web page www.dataprotection.gov.uk.

All staff using personal data within the School will be told the limits of their authority to use and disclose such information through their managers, performance development and the induction process.

The Chief Operating Officer (COO) is the School's Data Protection Officer. The COO ensures that:

- all purposes and disclosures are co-ordinated and consistent
- all new purposes are documented and notified to the Data Protection Commissioner
- all problems can be investigated thoroughly.

4. Data Quality and Integrity

The School will not collect data from individuals where that information is excessive or irrelevant in relation to the notified purpose(s).

Details collected will be adequate for the purpose and no more. Information collected which becomes (over time or by virtue of changed purposes) irrelevant or excessive will be deleted.

All departments will have to create working procedures, with standards that can be monitored, for managing data collection and updating of records.

Information will only be held for as long as is necessary for the notified purposes(s) - after which the details will normally be deleted.

Where details of individuals are stored for long-term archive or historical reasons and where it is necessary to retain the personal detail within the records, it will always be done within the requirements of the legislation.

The School will ensure, as far as is practicable, that the information held is accurate and up to date.

- It is the intention of the School to check wherever possible the details given.

- Information received from third parties (i.e. neither the individual concerned nor the School) will carry a comment indicating the source, where practicable.

Where a person informs the School of a change of their own circumstances, such as home address or non-contentious data, their record(s) will be updated as soon as possible.

Where the individual requests that information be changed and it is not possible to update it immediately, or where the new information needs to be checked for its accuracy or validity, a comment will be placed on the disputed record indicating the nature of the problem.

If the system does not allow the individual record to be marked in this way, departments will ensure that a manual record is made of the request and that it is processed within a reasonable time-scale.

Every effort will be made to reach an amicable agreement on any disputed data. Where this is not possible the School will implement its complaints procedure.

An internal investigation will be implemented if there is any alleged improper misuse of personal data by staff and appropriate action will be taken.

5. Technical and Organisational Security

The School has implemented appropriate security measures as required under the Data Protection Act 1998.

In particular:

- Unauthorised staff and other individuals are prevented from gaining access to personal information.
- Appropriate physical security is in place and all visitors have to report to reception areas to sign themselves in and out of the buildings.
- Staff are informed that a visitor has arrived to see them.
- Computer systems are installed with user-profile type password controls to ensure data is only accessed by authorised users, and where necessary, audit and access trails to establish that each user is fully authorised.
- In addition, employees are fully informed about overall security procedures and the importance of their role within those procedures.
- Manual filing systems are held in secure locations and are accessed on a need-to-know basis only.
- Security arrangements are reviewed regularly.
- All staff are informed and regularly reminded about the limits of their authority on disclosing information both inside and outside the School.
- Where details need to be passed outside the School, it will be done with the person's consent except where this is not possible or where it is required by law (Data Protection Act Exemptions such as crime prevention/detection, prevention of injuries etc.) or where it is in the person's vital interests.
- Any unauthorised disclosure will be dealt with under the School's disciplinary procedures.
- Redundant personal data will be destroyed using the School's procedures for disposal of confidential waste.
- In general, paper waste is shredded by outside certified contractors under local agreements and magnetic media (disks, tapes, etc.) are either electronically wiped or physically destroyed beyond recovery.

6 Subject Access/Subject Information Requests

Any person whose details are held/processed by the School has a general right to receive a copy of their own information.

There are a few exceptions to this rule, such as data held for child protection or crime detection/prevention purposes, but most individuals will be able to have a copy of the data held on them.

Where any information relates to an identifiable third party, other than the data subject, consent must be gained from that third party, before any information relating to them can be released.

The School has the right to make a charge of £25.00 for such requests.

Any codes used in the record will be fully explained, any inaccurate, out of date, irrelevant or excessive data will be dealt with under the procedures outlined in the section of this document on Data Integrity.

The School will reply to subject access requests as quickly as possible and in all cases within the 40 days allowed by the Data Protection Act.

Repeat requests will be fulfilled unless the period between is deemed unreasonable, such as a second request received so soon after the first that it would be unlikely for the details to have changed.

A subject access/information request should be submitted in writing wherever possible, this will ensure that the School has the required information to be able to conduct a data search and to fulfill the request.

In some cases, especially with requests not submitted on the correct form, further information may be required from the requester which may delay the start of the 40 day maximum time limit.

7. CCTV

The School records CCTV images at all of its main buildings for security and crime prevention purposes. The images are recorded, managed and information requests handled in accordance with the CCTV Code of Practice and the Data Protection Act 1998. A copy of the Code of Practice is attached as an Appendix to this policy.

8. Further Information, Enquiries and Complaints

The COO is the first point of contact on any of the issues mentioned in this policy document.

- The COO will be responsible for dealing with all internal and external enquiries.
- Where possible, requests for detailed information should be made in writing.
- All complaints should be written, dated and should include details of the complainant as well as a detailed account of the nature of the problem.
- The School will attempt to complete internal investigations within twenty one days and in every case the person will receive an acknowledgement as soon as possible after we receive the complaint.

Any complaints received relating to data protection issues will be investigated by the COO through the School's complaints procedure.

APPENDIX TO DATA PROTECTION POLICY

CCTV Code of Practice and the Data Protection Act 1998

The School's purpose or purposes for the use of CCTV are as follows:

- Prevention, investigation and detection of crime;
- Apprehension and prosecution of offenders;
- Public and employee safety;
- Monitoring security of our premises.

The School follows the Information Commissioners CCTV code of practice

Access to and disclosure of images to third parties

The images recorded by the School CCTV is restricted and carefully controlled, so that the rights of individuals are preserved. And to ensure that the chain of evidence remains intact should this be required for evidential purposes. The School also ensures that the reason for which we may disclose copies of the images is compatible with the reason or purpose for which we originally obtained these images.

Disclosure

Any request from a member of the public should be approached with care. We have the discretion to refuse any request for information unless there is an overriding legal obligation or information access rights.

Law Enforcement Agencies

If the School receives a request for an image for the purpose of prevention, detection, and investigation of a crime, by a Law Enforcement Agency, it is not obliged to provide the footage/information requested. However, the School should consider the request in the light of all the circumstances. The Police do have powers to seize the footage/information for investigative purposes under Section 29(b) of the Data Protection Act 1998 and Section 19 of the PACE Act 1984.

Access by data subject

This right is set out in Section 7 of Data Protection Act 1998. Requests for images or footage should be requested in writing.

Right of subject access by the Data Subject

On making a request in writing and paying the fee to the School, an individual is entitled to be told by the School whether they or someone else on their behalf is processing that individual's personal data.

If so, they are to be given a description of:

- the personal data,
- the purposes for which they are being processed and,
- those to whom they are or may be disclosed.

Freedom of Information Act 2000 (FOIA)

If an individual decides to request CCTV footage under the FOIA you should consider:

- Are the images those of the requester? If so, it is exempt under the FOIA and should be treated as a data protection subject access request.
- If the images are of other people they can be disclosed only if disclosing the information does not breach the DPA.

Companies requesting images

Under the DPA and FOIA, we are not legally obliged to disclose images, because the company is not the data subject and their purpose for requesting images is not tenable.