The Academy Trust of Melksham

Data Protection Policy

1.0 Scope

This Policy outlines how the ATOM and all of the schools within it, the members, trustees, Local governing bodies and all of their employees must meet the requirements of the Data Protection Act 1998.

This policy applies to all employees and any other person with access to personal or sensitive information processed by The ATOM. Further details concerning handling data is available on individual schools websites.

The policy covers the obtaining of personal data, its storage and security, its use and its ultimate deletion or disposal. The policy should be read in conjunction with our Code of Conduct.

2.0 Introduction

Everyone managing and handling personal information needs to understand their responsibilities in complying with the Data Protection Act 1998 (the Act).

This policy covers all personal data, however they are held, on paper or in electronic format, and the rights of individuals (data subjects) who wish to see information the Schools hold about them (by submitting a Subject Access Request). It is a legal requirement that the ATOM and the schools comply with the Act, and all members of staff have a statutory responsibility to ensure legal compliance.

This policy is intended to facilitate compliance and all staff should be aware of its content and the key requirements of the Act. The Code of Conduct also refers to staff obligations with regard to Data Protection and managers should ensure that staff are provided with the appropriate knowledge and training to ensure they can fulfil their responsibilities.

All of these documents are available on the website (atom.wilts.sch.uk). The Data Protection Officer (Chief Executive Officer) is responsible for making staff aware of these documents.

3.0 Responsibilities

Whilst the ATOM's Chief Executive Officer is ultimately responsible, both personal and corporate responsibility applies. All employees are therefore responsible for ensuring compliance with the Principles of the Data Protection Act by complying with this policy.

Line managers must ensure that those staff managing and handling personal information are adequately trained and supervised with regard to the requirements of this policy. The Headteacher in each school is responsible for ensuring that they and staff in their respective schools are aware of the relevant documentation. Headteachers will progress relevant Data Protection Subject Access Requests (See paragraph 12 below) and liaise with the ATOM Data Protection Officer on any issues which may arise.

The Academies' Data Protection Officer will monitor the ATOM's and the Schools compliance with the Act, ensure that the Data Protection Policy is implemented, advise and consult on responses to data Subject Access Requests and make regular reviews of this policy and associated documentation.

4.1 Definitions

Personal data is information which relates to the living individual who can be identified:

- From that data
- From that data combined with other information which is either in the ATOM or Schools' possession or likely to come into their possession.

For the purposes of the Act, and the Data Protection Policy, it is safest to assume that all information about a living, identifiable individual is personal data and should be dealt with accordingly.

Sensitive Personal Data can include information relating to:

- Religious belief
- Sexual life
- Physical or mental health conditions Member of a trade union
- Political opinions
- Commissions or alleged commissions of an offence
- Proceedings for any offence committed or alleged to have been committed.

Sensitive data must only be used for approved purposes (e.g. equal opportunities monitoring) and access to this data must be restricted to those who have a need to know. They should never be kept in a generally accessible record or file. Advice on the issue of sensitive data can be sought from the Data Protection Officer.

5.1 The Principles of the Data Protection Act 1998

The eight principles which form the basis of the Act state that data must be:

- **Fairly and lawfully processed:** Data must be processed fairly and lawfully. Nobody should be deceived or misled about the purpose for which their data is to be processed.
- **Processed for limited purposes:** Personal data can only be obtained for specified and lawful purposes with permission from the data subject for each purpose.
- **Adequate, relevant and not excessive:** The data must be sufficient to meet their purpose but not provide more information than the purpose requires, or provide information outside the scope of the purpose.
- **Accurate:** The personal data must be accurate when recorded, and accuracy must be maintained throughout the lifecycle of the data.
- **Not kept for longer than is necessary:** Personal Data must not be kept for any longer than is necessary for the purpose for which it is obtained. If data are kept for too long, the accuracy and relevance may be compromised.
- **Processed in line with the rights of the subject of the data:** Data subjects have the right to access their personal data and can request the termination of any processing that causes or is likely to cause them distress. They can insist that their data is not used for marketing and other purposes, and can request that inaccurate data amended.
- **Stored and processed securely:** All necessary measures must be taken to prevent unauthorised or unlawful processing of personal data and to protect personal data against loss, damage or destruction.
- **Not transferred to countries without adequate protection:** Personal data must not be transferred to a country outside the European Economic Area (i.e. the EU member states, Norway, Iceland and Liechtenstein) unless that country has in place a level of data protection comparable to that in the EU. Advice should be sought from the Academies' Data Protection Officer.

6.1 Processing Personal Data

The definition of processing in relation to data protection is very wide. Obtaining, holding, filing, organising, transmitting, retrieving, disseminating, disclosing and destroying of data are all deemed to be processing in addition to any other process that is carried out on the data.

Members, employees and others acting on behalf of the ATOM or Schools must only have access to personal data that are necessary in order to carry out their duties and responsibilities.

All forms used to obtain personal data, such as application forms or registration forms must:

- State the purpose/s for which the information is required.
- Be reviewed regularly to check that all of the information asked for is still required and necessary.
- Be checked for the accuracy of the data before they use for any processing. If in doubt about the accuracy of the data they should be referred back to the data subject for confirmation.

Personal data must be collected and handled in a way that complies with the Act and meets the eight principles above. This imposes a duty on the Schools to ensure that individuals are made aware of the uses that will be made of the information that they supply and give their consent to this.

If data are provided by an outside agency then the agency must be asked to confirm in writing that the data were obtained fairly and lawfully, in compliance with the Act.

Any information held regarding criminal convictions must be treated as sensitive information and handled accordingly. Any request made by the ATOM for such information must be fully justified. Advice should be sought from the Data Protection Officer.

Where personal data is provided for the purpose of placing a contract to which the data subject is a party then such data is considered to be fairly and lawfully obtained.

7.0 The Purpose of the Data

In addition to obtaining consent, the data must be used only for the declared purpose/s, which the ATOM have notified to the Information Commissioner's Office.

If there is a new purpose or change to an existing purpose then the Academies' Data Protection Officer must notify the Information Commissioner's Office Immediately.

Processing of data cannot begin for the new or amended purpose until the Commissioner has accepted this notification. The Academy registration entry with the Information Commissioner's Office can been seen via the intranet or from the Data Protection Officer.

8.0 Relevant and Adequate Data

The Academies must process only that information which is necessary to fulfil the business requirement or which is needed to comply with legal requirements. For example it is not necessary to ask about a driving licence on the job application form if the post applied for does not entail any driving duties.

9.0 Collective Accurate Data

Errors in personal data that cause data subjects damage or distress could lead to the ATOM being prosecuted. It is important therefore that all appropriate measures are put in place to verify the accuracy of data when they are collected, especially when any significant decisions or processes depend upon the data.

There is a requirement to ensure that data are kept up to date throughout the lifecycle of the data.

10.0 Keeping Data Only As Long As Necessary

Retentions periods should be defined for personal data and procedures put in place to ensure compliance.

Retention periods must be for clear business purposes and must be documented to identify why certain records are retained for certain periods of time.

When no longer required, data must be deleted or disposed of securely. Further information on this is available from the Data Protection Officer.

11.1 Safeguarding the Rights of Data Subjects

Individuals have various rights under the Act. These are:-

- The right to be told that processing is being carried out
- The right of access to their personal data
- The right to prevent processing in certain cases
- The right to have inaccurate or incorrect information corrected, erased or blocked from processing.

12.0 Subject Access Requests

The Schools must make available details of how individuals can request access to their data, by means of the Subject Access Request.

Subject Access Requests must be made in writing and sufficient detail must be obtained to ensure that the request had been made by the data subject in person.

As proof of identity at least two identifying documents of the data subject, such as a driving licence, passport, recent utility bill, etc. must accompany the request. If a third party is making the request, a signed letter of consent from the data subject should also be enclosed.

The request must then be passed to the Data Protection Officer to progress.

Subject Access Requests must be satisfied within 40 calendar days of their receipt by the Academies.

Some subject Access Requests may require further information before the process can commence. This information must be requested as soon as possible after the original request has been made. If this additional information is not received within 6 months, the request should be closed and a new request will have to be made.

It is not permitted to give personal data to third parties unless it is already in the public domain, or authorised by the data subject.

In certain circumstances, the courts, police and Inland Revenue may have the right of access to personal data without prior permission or knowledge of the individuals concerned. Any such request should be referred to the Data Protection Officer.

13.0 Keeping Data Secure

The Academy acts as custodian of personal data and must therefore ensure that necessary and sufficient precautions are in place to prevent misuse or unauthorised access to data as well as having security measures in place to prevent loss or damage to data.

Filing cabinets containing personal data must be locked outside of normal working hours and keys must be held securely by nominated staff.

Electronics files must be password protected. All electronic data must be encrypted.

All such electronic data must be stored in secure server areas, if on computer hard drives, laptops or other mobile devices the devices must be protected by passwords .

Any electronic data backed up to media such as CD must be kept physically secure.

If any data are to be taken from the office (e.g. to work at home) then the data must be held securely at all times whilst in transit and at the location they are being held. In particular data must be protected from unauthorised access.
Where outside bodies process or hold any of the Academies' personal data then the Academies must be satisfied that the data is held securely and with due regard to the obligations of the Act.

14.0 Transfer of Data

Data must not be transmitted or transferred out of the European Economic Area (i.e. the EU member states, Iceland, Norway and Liechtenstein) unless the country they are being transferred to has the same or equivalent standards of Data Protection. This has implications for data placed on the Internet and use of e-mail where servers are based abroad.
If information is required to be transferred abroad then checks must be made to ensure that the data is held securely during transfer and that data recipients apply data protection rules equivalent to those in the UK Data Protection Act 1998. Advice on this should be sought from the Academies' Data Protection Officer.

15.1 Links to other Academy Policies

This policy should read in conjunction with the following related policies:

- Capability and Disciplinary
- Code of Conduct
- Freedom of Information
- Grievance
- Health and Safety
- Internet and ICT Usage