Tamworth Enterprise College
An AET Academy
To make our best better

DATA PROTECTION POLICY

"Further advice and guidance on this policy can be obtained from the Group's Professional Services Business Intelligence Team"

Contents

1. POLICY STATEMENT

1.1 Throughout this document "the Group" will refer to Academies Enterprise Trust (including Professional Services), London Academies Enterprise Trust, Unity City Academy Trust or individual academies as appropriate.

1.2 The Group needs to collect, store, use and share personal information about pupils, employees and other individuals in order to deliver services, exercise its responsibilities and duties of care as an employer and provider of education. In doing so the Group must comply with the Data Protection Act (1998). This law requires the Group to protect personal information and control how it is used in accordance with the legal rights of the data subjects – the individuals whose personal data is held.

1.3 This policy recognises the need to treat that information in an appropriate and lawful manner and aims to ensure the Group complies with its obligations as a Data Controller. It sets out the rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

1.4 This policy has been approved by the Board and will be reviewed every two years or as required.

2. INTRODUCTION

The objective of this policy is to enable the Group to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice in relation to the collection, processing and storage of personal data;
- provide guidance and support to all employees handling information on behalf of the Group;
- protect the Group from the consequences of any breaches of their responsibilities.

2.1 The Data Protection Act 1998

The Act came in to force on 1 March 2000 and applies to anyone who collects, processes, stores or is the subject of personal data. The Act works in two ways:

- Anyone who records and uses personal information (data controllers) must be open about how the information is used and must follow the eight principles of the Data Protection Act (1998).

- All individuals (data subjects) have the right to see what information is held about them and the right to have information corrected if it is wrong.

Misuse of personal data, whether accidental or deliberate loss or disclosure to third parties, presents significant legal, financial and reputational risks including fines of up to £500,000 for serious breaches.

2.2 Scope of Policy

This policy applies to Trustees, local governors, employees, contractors and volunteers working within the Group. It applies to all personal data that the Group hold. Personal data means information relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Group.

The Act applies to personal data, including all information in pupil and employee records:

- held on a computer or other automated system;

- held on a structured filing system (paper or manual);
- visual data such as photographs, video clips (including CCTV) or sound recordings.

For example, personal data could be name, data of birth, address, NI number, medical records, exam results, SEN assessments or employee development reviews.

Sensitive personal data is a separate category in its own right and there are greater responsibilities when gathering information on:

- health details;
- ethnicity;
- sexuality;
- religion;
- criminal offences;
- political opinion;
- trade union membership.

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.

2.3 Relationship with existing policies and guidance

This policy has been formulated within the context of the following documents:

- Data sharing protocol;
- Working alone policy;
- Acceptable use agreement;
- Password policy;
- E-safety charter;
- Records management toolkit;
- Guidance for issuing privacy notices;
- Website-terms of use;
- Social media and networking policy;
- Additional guidance for academies on responding to subject access requests.

3. DATA PROTECTION PRINCIPLES

Whenever employees, contractors or volunteers 'process' personal data, they must comply with all the Data Protection principles and in doing so achieve the aims of protecting individuals from harm. The Data Protection Act 1998 has eight principles; these principles are legally enforceable and are summarised below:

1. data 'processing' must be 'fair' and legal;
2. data must be obtained only for specified purposes(s) and used only in ways that are compatible with the purpose;
3. data must be adequate, relevant and not excessive;
4. data must be accurate and up to date;
5. data not be not held for longer than necessary;
6. data subjects' rights must be respected;
7. appropriate security must be in place to protect and store data;
8. data shall not be transferred outside of the European Economic Area unless that country or territory ensures an adequate level of protection.

4. NOTIFICATION

The Data Protection Act (1998) requires every data controller who is processing personal data to notify and annually renew a notification to the Information Commissioners Office (ICO). The ICO maintains the public register of all data controllers. The ICO register can be consulted by individuals to find out what processing of personal data is being carried out by a particular data controller. Failure to comply is an offence.

The Group is registered under three notifications with the Information Commissioner's Office (ICO):

- Z1528259 (Academies Enterprise Trust)
- Z2472046 (London Academies Enterprise Trust)
- Z9069322 (Unity City Academy Trust)

The Group's Professional Services Data Team is responsible for renewing the notifications. Individual academies do not need a separate notification.

5. PRIVACY NOTICE

To comply with the Data Protection Act (1998), a Privacy Notice must be issued to data subjects i.e. pupils/parents and employees to inform them of the purposes for which personal data is collected, held and used. The Group has two Privacy Notice templates; one for the academy workforce and one for pupils/parents.

6. RESPONSIBILITIES

6.1 AET Board and CEO

The Board have ultimate accountability for the Group's compliance with data protection law. The CEO is accountable for implementing the policy on behalf of the Board.

6.2 The Director of ICT

The Group's Professional Services Director of ICT is responsible for ensuring that centrally managed IT systems and services take account of relevant data protection risks and for promoting good practice in IT security among relevant employees.

6.3 The Director of HR

The Group's Professional Services Director of HR is responsible for reviewing relevant human resources policies and procedures, in order to support managers and employees in understanding and discharging their responsibilities for data protection through the recruitment, induction, training, promotion, discipline and leaver management processes.

6.4 Principals/Headteachers and Managers

Principals/headteachers and managers are responsible for:

- Ensuring compliance of policy within the day-to-day activities of their academy or Professional Service's team;
- Ensuring that the policy is brought to the attention of all employees and that all employees receive appropriate training;
- Reporting any major breaches or risks in data protection to the Group's Professional Services Data Team;
- Ensuring that employees, contractors, consultants and volunteers have access only to such personal data that is necessary for them to fulfil their duties.

6.5 Employees

Employees are responsible for:

- Adhering to the terms of this policy;
- Ensuring that all personal information entrusted to them is kept securely;
- Ensuring no personal information is disclosed to any unauthorised third party;
- Ensuring that their own personal data held by the Group is kept up to date.

A breach of this policy could, potentially, be considered gross misconduct and subject to disciplinary procedure.

7. COMPLIANCE AND MONITORING

The Board and Academy Principals/Headteachers will monitor compliance of this policy by ensuring that:

- The Board will regularly monitor compliance with this policy through the Audit & Risk committee;
- There is someone with specific responsibility for data protection;
- Everyone managing and handling personal data understands that they are contractually responsible for adhering to the eight principles;
- Everyone managing and handling personal data are appropriately trained to do so using the the AET data protection toolkit;
- Everyone managing and handling personal data are appropriately supervised when necessary;
- A review and audit is conducted of the way personal data is handled, as well as the effectiveness of this policy;
- Methods of handling personal information are assessed and evaluated;
- Everyone managing and handling personal data understands where to go for enquires, advice, guidance and good practice on data protection.

8. ACCESS TO INFORMATION

The Data Protection Act (1998) gives all individuals about whom the Group hold personal information the right to access information that relates to them whether it is held electronically or in manual form. Although the Act refers to structured manual filing systems, access to information held in an unstructured filing system may also be requested.

8.1 Pupils Rights

Pupils have a right of access under the Data Protection Act (1998) to their own information. This is known as the right of subject access. When a child cannot act for themselves or the child gives permission, parents will be able to access this information on their behalf. The Information Commissioner's Office (ICO) advises that as a general guide, a pupil of aged 12 or older is expected to be mature enough to make a request. A pupil may request their 'educational record'. Broadly speaking, this expression has a wide meaning and includes most information about a pupil that is processed by or on behalf of an academy. However, information kept by a teacher solely for his or her own use does not form part of the educational record.

Appropriate staff within an academy should judge whether the request is in the pupil's best interest and whether the pupil will understand the information provided. Staff may also wish to consider whether the request has been made under coercion.

In some circumstance, academies can withhold information where the information might cause serious harm to the physical or mental health of the pupil or another individual.

8.2 Parent or Legal Guardian Rights

Under the current legislation, a parent or legal guardian has no legal right to access a child's education record if their child attends an academy, unless they are doing so on behalf of their child. Therefore it is up to the Principal/Headteacher to decide whether to grant such access, and it is likely to depend on the relationship between the parent and academy.

8.3 Employee Rights

Employees have a right to request access to their own employee records.

- Employees within AET Professional Services should direct all subject access requests to the HR helpdesk;
- Employees working in academies should direct all subject access requests to the Principal/Headteacher in the first instance.

8.4 Dealing with Access Requests

Requests need to be received in writing (or email) and the appropriate person dealing with the request needs to be satisfied as to the identity of the person making the request. Proof of identity, confirming name and address, should be requested for this purpose. The request does not have to be in any particular form. Nor does it have to include the words 'subject access'.

The time limit for providing information pursuant to a subject access request is 40 days.

A fee may be charged for dealing with a subject access request. If this is done, there is no need to comply with the request until the fee has been received. The maximum fee that can be charged is normally £10. However if a subject access request is made for information in a pupil's 'educational record' then the maximum charge is £50.

Detailed guidance about subject access requests can be found on the ICO website.

8.5 Disclosures to the Police

Disclosures to the Police are not compulsory except in cases where served with a Court Order requiring information. Requests from the Police for access to information must be made in writing via Section 29(3) of the 1998 Data Protection Act. The Police must complete a form, which should then be approved by the Group CEO. Details of how to access the form are outlined in the appendix.

Employees must not release information to the Police over the telephone. In cases where a request from the Police has been made but a Court Order is not served, consideration must be given to the implications of disclosure before any action is taken. The Group may be required to provide an explanation for any disclosure of the data subject's personal information at a later date and must be able to provide justifiable reasons for doing so e.g. where the Academy believes that failure to release the information would prejudice an investigation.

9. GUIDANCE AND GOOD PRACTICE PROCEDURES

The guidance that follows addresses the minimum standards and responsibilities for all employees handling personal data. Where guidance is outside the scope of this document, information relating to other polices will be clearly provided.

Security measures will vary according to type of software used at academies and by Professional Services teams, building security, type and amount of data and whether employees are working from home or alone off site. Principals/Headteachers or managers should assess whether additional guidance needs to be provided in order to cover potential security risks or data protection breaches.

9.1 Data Collection (Principle 1, 2, 3 & 4)

Taking the right steps at the point of data collection is probably the most important step in achieving compliance. Providing clear information to data subjects i.e. issuing a Privacy Notice is the key factor in obtaining and processing data fairly. Raising awareness of the commitments and compliance to the Data Protection Act (1998) can be assisted with tools such as employees handbooks, academy prospectus and website or information displays and notices.

The minimum standards during data collection are to:

- Ensure that data subjects are aware of the identity of the Data Controller;
- Inform data subjects of why information is being collected and how it will be used;
- Check that the data subject has given explicit consent;
- Ensure that data subjects have not been misled or deceived during the process of data collection, especially if information has been gathered from a third party;
- Check that data is fit for the purpose for which it will be used. This means obtaining good quality data;
- Check that data is accurate and up to date so as to present a fair picture of circumstances. Verification procedures during data collection should be as close as possible to point of data entry;
- Take, where possible, reasonable steps to ensure the accuracy of data, especially if obtaining information from third party sources. Use every opportunity of contact with the data subject to ensure that information is correct or set regular schedules to audit data;
- Use personal data only for purposes that are compatible with the original purposes for which the data was collected. Any other use amounts to unlawful processing;
- Ensure when photographs or video recording of employees and/or pupils, as individuals or small groups are taken that the individual(s) concerned have given consent and understand how the images will be used;
- Notify pupils, visitors and employees with signs indicating why CCTV is in use and only keep the footage for a set period of time. Capturing images of identifiable people means the data protection principles apply to CCTV and subject access requests can be made;

9.2 Data Storage and Security (Principle 1, 5 & 7)

Taking the right steps to protect and store personal data can ensure that no harm is caused to data subjects, employees and the reputation of the Group.

The minimum standards data storage and security are to:

- Ensure technical measures are in place to prevent accidental compromise and damage during the storage, use and handling of personal data;
- Restrict access to buildings and offices as appropriate;
- Keep desks and filing cabinets locked when not in use;
- Never leaving printed personal data on desks, notice boards or tables where there is general access;
- Keep portable electronic devices secure both on and off work premises and keep them locked up when not in use;

- Use strong passwords to access electronic devices and encrypt personal devices and removable media;
- Be vigilant when transporting electronic devices, especially with smaller devices such as memory sticks;
- Follow guidelines for secure disposal or shredding of paper and/or other tools of data storage;
- Report suspected security beaches immediately to appropriate employees;
- Ensure employees understand and are trained to use data collection systems accurately;
- Follow retention policy and check that data is not kept for longer than is necessary;
- Understand that if data processing is handled by a third party e.g. a pupil assessment tracking software company, paper shredding company then the Group is still responsible for data processing done by a third party. A written agreement i.e. contract should be in place that includes details of data security;

Note that if employees use their own personal devices for work then they must be secure. If an employee leaves the Group or sell their device then the Group remains responsible for personal data relating to the Group on the device.

9.3 Data Sharing and Disclosure (Principle 1, 6 & 8)

Taking the right steps to protect how personal data is shared and disclosed will reduce the risk of unauthorised access and ensuring compliance when exchanging information. It will also minimise the risk of breaking the law and avoiding complaints or disputes about how personal data is shared.

The minimum standards on data sharing and disclosure are:

- Data should only be shared with employees, contractors or third parties who need it in order to carry out their normal duties;
- Personal data held within the Group can be disclosed to employees who need to know it in order to carry out their normal duties;
- Data should only be disclosed or shared after the identity of the personnel or organisation has been verified;
- The risk for sharing personal data should be evaluated and monitored. An assessment should be made as to whether the objective can be achieved without sharing the data;
- Data should be anonymised before sharing where appropriate;
- Privacy notices are clear, relevant and shared with data subjects;
- Ensure that data shared with other organisations, third parties are noted on the Privacy Notice;
- Information is accurate before sharing;
- Employees are trained to ensure they understand who has the authority to share personal data with third party organisations and what checks, circumstances should be verified before sharing;
- Circular emails to parents or professionals should be sent bcc (blind carbon copy) so that email addresses are not disclosed to everyone;
- Excessive or irrelevant information is not shared;
- Ensure that systems for sharing are not incompatible. This can lead to loss, corruption or degradation of data;
- Keep information secure when it is passed on and that it will be kept secure;
- Personal data can be disclosed to a third party e.g. Local Authority if it is listed in the Privacy Notice or the data subject has given specific consent;
- Requests from third parties are often made by telephone, with the added problem of verifying the identity of the caller. Even when the call appears to be genuine, data should not be

disclosed unless the organisation is listed in the Privacy Notice and the identity of the caller has been verified. If this not the case, an offer should be made to contact the data subject concerned, on behalf of the caller, or to pass on a message;

- Check how the recipient is recording the information to avoid records being mismatched or becoming corrupted. Assess whether information is recorded in a common or different format e.g. date of birth can be recorded in various different arrangements;
- Ensure that electronic files are password protected and emailed via secure servers;
- Check the electronic delivery method will not corrupt files so that information is lost or inaccurate.

10. APPENDIX

10.1 The Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) is an independent authority in the UK that promotes openness of official information and protection of private information. The ICO's role is to uphold information rights in the public interest.

The Data Protection Act (1998) requires every organisation that processes personal information to register with the Information Commissioner's Office, unless they are exempt. Failure to do so is a criminal offence. There are a number of tools available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. These include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller.

There are more than 370,000 registered data controllers. ICO publish the name and address of these data controllers, as well as a description of the kind of processing they do. A search of the register can be made by visiting the ICO website: https://ico.org.uk/esdwebpages/search

Contact details for Information Commissioner's Office Head Office:
Wycliffe House Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113 (local rate)

10.2 Glossary of Terms

Data Protection Terms	Definitions
Data	Data means information which – (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).
Personal Data	Personal data means data which relates to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Sensitive Personal Data	Sensitive personal data means personal data consisting of information as to - (a) the racial or ethnic origin of the data subject, (b) his/her political opinions, (c) his/her religious beliefs or other beliefs of a similar nature, (d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his/her physical or mental health or condition, (f) his/her sexual life, (g) the commission or alleged commission by him/her of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.
Data Subject	Data subject means an individual who is the subject of personal data.
Data Controller	Data controller means a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

	In relation to data controllers, the term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other.
Data Processor	Means any person or organisation (other than an employee of the data controller) that processes the data on behalf of the data controller.
Recipient	Any person to whom the data is disclosed.
Processing	Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including – (a) organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.
Register	A public register of data controllers maintained by the ICO.
Third Party	In relation to personal data, means any person other than – (a) the data subject, (b) the data controller, or (c) any data processor or other person authorised to process data for the data controller or processor.

10.3 AET Data Protection Toolkit

This policy along with a range of training videos and a quiz can be found on the AET Comms Portal, under Data Intelligence > Data Protection. All new employees and individuals within the scope of the policy are requested to watch the videos, read the policy and take the quiz within the first 4 weeks of joining the Group. The results of the quiz are recorded centrally and provide a way to audit compliance towards the policy. All employees must read the policy every 12 months and re-take the quiz.

10.4 Section 29: Police Request for Disclosure

The template for police requests can be found on the Comms Portal under Data Intelligence>Data Protection. The document is called 'Data Protection Form'. All completed forms must be forwarded on to the CEO.