THE EDUCATION ALLIANCE

Data Protection Policy

Version 1.0

Important: This document can only be considered valid when viewed on the VLE. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online. **Name and Title of Author:**	
Name of Responsible Committee/Individual:	Trust Board
Implementation Date:	9/2/2017
Review Date:	Spring 2019
Target Audience:	All stakeholders
Related Documents:	Acceptable Use Policy Email and Electronic Communications Policy Freedom of Information Act 2000 Publication Scheme CCTV Policy FOI Policy
References:	www.ico.org.uk

Contents

Appendices

1. POLICY STATEMENT

The Education Alliance understands its obligations under the Data Protection Act 1998 (the Act) and takes those responsibilities seriously. The Act regulates the use of personal data and this policy aims to inform staff of their responsibilities, ensuring that employees adhere to the Act, minimising the risk of unintentional breaches.

2. PURPOSE AND SCOPE

The Education Alliance has a diverse workforce and staff in various roles that will come into contact with and use confidential personal information about people (e.g. students, their families, staff and other stakeholders) on a regular basis. The Education Alliance also holds information about every member of staff and staff are required to inform the Human Resources Department of any relevant changes to ensure information retained is accurate (e.g. address, contact details, bank details).

3. AIMS & OBJECTIVES OF THE POLICY

The Education Alliance aims to adhere to the Act in an honest transparent way, therefore staff, students and other stakeholders should be made aware of the types of personal information the School retains in relation to them, the way in which the information will be stored, used, shared and destroyed.

The Act requires eight data protection principles are followed in the handling of personal data, requiring personal data to be:

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate
- Not retained for longer than is necessary
- Kept safe and secure
- Processed in accordance with the rights of data subjects under the Act
- Not transferred to countries outside the European Economic Area without adequate protection

There is stronger legal protection for more sensitive information, such as ethnic background, political opinions, religious beliefs, health, sexual health and criminal records.

It is vital that staff are aware of their own responsibilities for data protection and that they adhere to them, seeking advice from the IT Manager or the Human Resources Department when they are unsure.

4. ROLES AND RESPONSIBILITIES

The **Trust Board and Local Governing Body** will ensure that appropriate policies, procedures, systems and processes are in place within the Trust and each of its schools to minimise the risk of a breach of the Act.

The **CEO** is responsible for ensuring that staff are aware of the expectations surrounding data protection and the potential consequences should a breach occur.

The **Director of Human Resources** will ensure that freedom of information and subject access requests are managed appropriately and within specified timescales and parameters, providing others with advice and guidance where required.

The **Human Resources Department** is responsible for developing, reviewing, monitoring and circulating appropriate policies, documentation and information to staff in relation to the Act.

The **IT Department** is responsible for ensuring that electronic data systems adhere to the requirements of the Act and that there are appropriate mechanisms in place for monitoring and access, such as audit trails, access rights, password and security measures and IT related policies and procedures.

All **staff** are responsible for ensuring they familiarise themselves with the related policies, procedures, guidance, systems and processes, as well as ensuring that they adhere to The Education Alliance's expectations (e.g. utilising passwords appropriately, using encrypted electronic portable storage devices, storing information in line with requirements, responding to requests for information appropriately and ensuring personal data is not placed at risk of inappropriate access).

5. GENERAL EXPECTATIONS

It is expected that staff familiarise themselves with the Expectations and Code of Conduct document, alongside other policies, procedures, advice and guidance related to their particular roles within The Education Alliance. Passwords must not be shared and accessing personal records without authority will be viewed as potential gross misconduct (it may also be viewed as a criminal offence).

When transmitting confidential information by electronic methods:

- Only transmit information between locations using a secure network or comparable arrangements. Encryption may also be useful.
- Ensure that all copies received are held securely (e.g. that they are saved on a file that has limited appropriate access or is encrypted).

It is vital that staff read, understand and adhere to the IT policies (e.g. Acceptable Use Policy and Email and Electronic Communications Policy).

Student and employee data must not be transferred to countries outside the European Economic Area (EEA) unless:

- the destination country has been designated as providing adequate protection by the European Commission
- the destination country is the US and the recipient has signed up to the ‘safe harbour’ principles
- the employee/student concerned has been told about the intended transfer and has agreed to it
- the transfer is to an organisation that acts only as a processor, the processor is reliable, the country in which it is located is stable and the required controller-processor contract is in place
- steps have been taken to ensure that, taking account of all the circumstances of the transfer and the Information Commissioner’s guidance on international transfers, adequate protection is provided in other ways.

Should The Education Alliance be required to transfer any data relating to staff (e.g. under the terms of the Transfer of Undertakings (Protection of Employment) Regulations 1981 (TUPE), the data transfer will meet the TUPE requirements.

The Education Alliance will monitor emails, telephone calls and website access in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

In relation to the retention of records, The Education Alliance follows the retention periods recommended by the Information Commissioner, which include the following for staff:

- Application form for the duration of employment
- References for 1 year
- Payroll and tax information for 6 years
- Sickness records for 3 years
- Annual leave records for 2 years
- Unpaid/special leave records for 3 years
- Annual appraisal/assessment records for 5 years
- Records relating to promotion, transfer, training and disciplinary matters for 1 year following the end of employment
- References/information to enable references to be given – 5 years following the end of employment
- Summary of record of service for 10 years following the end of employment
- Records relating to accident or injury at work for 12 years

There are also specific timeframes relating to areas such as safer recruitment and the education sector. The Information Commissioner’s report on data protection for schools 2012 includes a summary of the main recommendations as follows:

- The Information Commissioner’s Office (ICO) must be accurately notified of the school’s processing of personal data
- The school must recognise the need to handle personal information in line with the data protection principles

- Students and staff should be advised of the way in which their personal information will be processed
- Confidential information must be stored, used and shared securely
- When disposing of records steps must be taken to ensure that personal information cannot be retrieved
- The School must have clear, practical policies and procedures on information governance for staff and governors and their use and effectiveness should be monitored
- Subject access requests should be logged, responded to and monitored as appropriate
- Before data is shared with others, steps should be taken to ensure the school is allowed to share the information and that it will be kept securely
- Personal information, including images, have appropriate website access security in place
- Staff and students are informed about CCTV in operation (e.g. its use and retention periods)
- If the School intends to take photos for publication, the school's intentions must be shared in the fair processing/privacy notice
- The school must recognise when personal data will be processed by others and steps must be taken to ensure that it is processed securely
- Staff and Governors must have access to appropriate basic training regarding data protection
- A Freedom of Information framework must be established at the School to ensure that requests are responded to appropriately

6. INFORMATION COMMISSIONER

The Education Alliance has a responsibility to notify the ICO that it processes personal data, confirming the name(s) of the data controller(s) within the organisation. Where changes occur (e.g. CCTV usage) the school should notify the ICO.

The ICO defines personal data as information which related to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that details something about an identifiable living individual. The principles also extend to all information in education records (e.g. names of staff and students, dates of birth, addresses and SEN assessments).

Sensitive personal data is defined as information that relates to race and ethnicity, political opinions, religious beliefs, membership of a trade union, physical or mental health, sexuality and criminal offences. The difference between processing personal data and sensitive personal data is that there are greater legal restrictions on the latter.

It is vital that information retained by The Education Alliance is secure as the loss of information or unauthorised access to personal information can cause harm to students, their families and staff. A breach of information security can result in a monetary penalty from the ICO and individuals can also seek compensation, which can impact on reputational risk and issues of trust and confidence. The Education

Alliance regularly reviews its physical security (buildings and storage systems) which includes storage of paper records and access to them, as well as electronic systems and access issues. Theft of a hard drive or damage to a router or server can seriously affect business continuity. Procedures are in place to ensure portable electronic devices are secure both on and off school premises and access to personal data is limited to reduce the potential of inappropriate access.

7. SUBJECT ACCESS REQUESTS

Individuals have the right to request the personal information The Education Alliance holds about them and this is called a Subject Access Request. The definition extends to any personal information held on record anywhere by the school. Subject Access Requests (SARs) must be answered within 40 calendar days of receipt and the school can charge a fee (the standard charge is £10 per request). A valid SAR should be lodged in writing and the school should confirm the requester's identity prior to responding. Parents can make a subject access request on their children's behalf if their child is deemed too young to look after their own affairs or if the child has given their consent.

8. SHARING INFORMATION

There will be times where it is appropriate that The Education Alliance shares information with other organisations, such as the Local Authority, other Schools and educational establishments and Social Services. Personal information can be shared with students once they are old enough to be considered responsible for their own affairs, although information can also be shared with their parents and guardians.

The three most important aspects to consider when sharing data are:

- Ensuring the school is allowed to share it
- Ensuring there is adequate security in place
- Providing an outline in a fair processing notice detailing who should receive personal information from the School

Before sharing information, consideration must be given to how the information will be shared (e.g. via a secure server with recipient's arrangements in place that are secure). Documents may require password protection and care should be taken to ensure that the information is being sent to the correct place and person (e.g. if it is via an email, check that the email address is accurate).

9. USE OF BIOMETRICS

The Department for Education has advised that the duties on schools in the Protection of Freedoms Act 2012 come into effect from 1 September 2013. This means that where The Education Alliance uses automated biometric recognition systems, it must ensure that staff, parents and students are appropriately informed and that consent is obtained. An alternative arrangement is made available if they do not wish to use a biometric system to access services.

10. MONITORING AND COMPLIANCE WITH AND EFFECTIVENESS OF THIS POLICY

Compliance and effectiveness of this policy will be monitored by the Human Resources Department.

11. REVIEW

This policy will be reviewed in partnership with recognised trade union partners within 2 years of the date of implementation.

Appendix 1

Checklist

Action	Lead	Status
Fair processing		
Provide parents and students with a fair processing or privacy notice, advising them of the personal information the school collects and why (including the purpose and use of CCTV and photos).		
Control access to personal information. Giving access only to people (e.g. staff and governors) that need the information to do their jobs and only when they need it. Ensure systems and procedures control access to paper and electronic records containing personal information.		
Information Security		
Regularly review the physical security of buildings and storage systems and access to them.		
Ensure all portable electronic devices are kept as securely as possible on and off school premises.		
Ensure procedures are in place and adhered to for circumstances where personal information is taken away from school premises in electronic or paper format.		
Strong passwords (e.g. at least 8 characters long and containing special symbols) should be encouraged alongside regular prompts to change passwords.		
Memory sticks are easy to lose or mislay. They should either not be used to hold personal information or they should be password protected and fully encrypted.		
Personal information should not be held on private electronic equipment as the school has no control over its security and disposal.		
Wherever possible, storage rooms, strong cabinets and other storage systems should have locks.		
Personal information should not be left on desks in offices or classrooms and particular care must be taken if personal information is taken out of school.		
Disposal		
The method of destruction of personal data should take into account the nature of the		

information. Ensure it is disposed of in a way that creates little risk of an unauthorised third party using it.		
Policies		
Ensure the school has clear and practical policies and procedures in all areas that affect good information governance.		
Subject Access Requests		
Subject Access Requests (SARs) need to be answered within 40 calendar days of receipt and a valid SAR should be in writing. The school should confirm the requester's identity before responding.		
The Governance Clerk should be notified of all SAR to ensure there is a log of all requests retained.		
Sharing Personal Information		
The main organisations schools share information with are Local Authorities, other schools and educational bodies and social services.		
When sharing data make sure you are allowed to share it; ensure that adequate security is in place to protect it and; provide an outline in a fair processing notice of who receives personal information from the school.		
If personal data is being shared via email, check that the recipient's arrangements are secure and consider password protecting the data (sending the password separately). Check the email address is correct and that you are only sending the information you need to send.		
Websites		
Do not disclose personal information (including photos) on a website without the individual student, member of staff or governor being aware. It is advisable to get consent prior to publishing photographs on a website.		
If sections of the website are user name and password controlled, ensure only the necessary level of access is given.		
Be wary of metadata or deletions that could still be accessed in documents and images on the website.		
CCTV		
Be clear with the ICO, staff, students and parents about the use of CCTV (e.g. why it is used and how).		

Site cameras should only be situated where they are needed for their stated purpose and where they do not unnecessarily intrude on anyone’s privacy.		
Have a set retention period based on the possible need to review the footage and consider who is allowed to access the footage and why.		
Photographs		
Schools can take photographs for inclusion in a printed prospectus or other school publication without specific consent as long as they school has indicated its intentions.		
Parents taking photographs of their children are not covered by the Data Protection Act.		
Processing by Others		
The school remains responsible for any processing of personal information a third party does on behalf of the school.		
Freedom of Information (FOI)		
The Trust has an FOI Policy and all FOIs should be logged with the Governance Clerk.		