

# Atlantic Centre of Excellence Multi Academy Trust

## DATA PROTECTION POLICY

<b>Date Adopted:</b>	<b>11 March 2016</b>
<b>Date to be Reviewed:</b>	<b>2 years</b>

### Contents

#### Introduction

#### Section 1 - Managing Data and Data Quality

1.1 Fair Collection & Processing

1.2 Registered Purposes

1.3 Data Integrity

1.4 Data & Computer Security

1.5 Procedural Security

#### Section 2 - Processing Subject Access Request

#### Section 3 – Enquiries & Further Information

## **INTRODUCTION**

Atlantic Centre of Excellence Multi Academy Trust (ACE MAT) collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the Trust. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Trust complies with its statutory obligations.

The Trust will ensure that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Trust intends 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 are aware of their duties and responsibilities within these guidelines.

In this document when we talk about a '**data subject**' we mean an individual who is the subject of the personal data or the person to whom the information relates. The term '**processing**' means obtaining, recording or holding the information or data. In all cases the term '**personal data**' will mean data which relates to a living individual who is identifiable.

## **SECTION 1**

### **1.1 Fair collection and processing**

ACE Multi Academy Trust takes its responsibility for collecting and using personal data very seriously and undertakes to do so both fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. Wherever possible, information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

### **1.2 Registered purposes**

The Data Protection Registration entries for the Academy Trust are available for inspection, by appointment, at the ACE Business Office.

Explanation of any codes and categories entered is available from the person nominated to deal with Data Protection issues in the Trust, or in each individual academy (see Appendix). Registered purposes covering the data held at the academy are listed on the academy's Registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subject's consent.

### **1.3 Data integrity**

The Trust 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 Trust or one of its academies of a change of circumstances their computer record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the Trust or academy will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Trust Directors for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

### **Data adequacy and relevance**

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the Trust or individual academies will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. Staff/pupil data is checked annually to ensure accuracy.

### **Length of time**

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the nominated person to ensure that obsolete data is properly erased. The Trust has its own Records Management Policy which will explain this in further detail.

### **Authorised disclosures**

The Trust and individual academies will, in general, only disclose data about individuals with their consent.

However there are circumstances under which the Trust's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the academy to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the academy.
- Staff data disclosed to relevant authorities eg in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the academy. Officers and IT personnel working on behalf of the LEA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the academy by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **needs to know** the information in order to do their work. The academy will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

## **Websites and Social Media**

On Trust websites or social media (for example, Facebook) we will ensure that we do not publish personal information (including images) without permission from the individual concerned. Access to websites and Facebook groups will be monitored by the Trust or individual academies on a regular basis.

## **CCTV**

Images of people are covered by the Data Protection Act, and so is information about people which is derived from images – for example, vehicle registration numbers. Where CCTV is used on Trust premises we will ensure that we tell people if it is in use.

### **1.4 Data and computer security**

What is a 'data and computer security'?

A key responsibility for anybody that has responsibility to keep data is how securely it is kept. Breaches (losses) of personal data can mean huge monetary fines being levied against the Trust where loss of the data has been due to a security breach or as a result of physical loss of information. Breaches in data can also mean a loss of confidence in the Trust and reputational damage. We always seek guidance on system security to ensure that we handle information safely.

We take into account what the risk of losing or not appropriately handling data may be – for example a potential risk of harm, hacking of academy systems, financial penalties – and ensure your systems “match” that level of security.

The Trust undertakes to ensure security of personal data by the following general methods such as:

#### **Physical security**

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed access to personal files. Information will be locked away securely when not in use. Visitors to the Trust and its academies are required to sign in and out, to wear identification badges whilst in the academy and are, where appropriate, accompanied.

#### **Logical security**

Security software including firewalls are installed on all computers containing personal data and are updated on a regular basis. Where needed, mobile devices, including phones, memory sticks, cloud technologies and laptops are also encrypted. Only authorised users are allowed access to the computer files. Computer files are backed up (i.e. security copies are taken) regularly. Access to computer systems are password controlled and these passwords are changed regularly. Passwords are not shared with another person and are unique to the user.

## 1.5 Procedural security

This is about having processes in place to ensure that all staff are not only aware of Trust academy policy, system security or what to do if they receive a request for information but also that they have clear and defined procedures which they can follow. Training for all staff is recommended and the Information Commissioner has a free e-learning training package on their site which we recommend all Trust staff undertake: please visit [www.bobs-business.co.uk](http://www.bobs-business.co.uk).

All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security for data is determined by the Trust Board and is monitored and reviewed regularly, especially if a security breach becomes apparent.

Any queries or concerns about security of data in the Trust or individual academies should in the first instance be referred to the nominated person (Appendix 1).

Individual members of staff can be personally liable in some circumstances in law under the terms of the Data Protection Acts. They may be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

## SECTION 2

### Processing a Subject Access Request

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 due to lack of capacity for example or the child gives explicit permission, parents will be able to access this information on their behalf.

#### **As a parent, what sort of information can I access?**

You have a right to access your child's educational record. This covers information that comes from a teacher or other employee of a local authority or academy, the pupil or you as a parent, and is processed by or for the academy's governing body or teacher, except for information the teacher has solely for their own use. So it will cover information such as the records of the pupil's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists engaged by the academy's governing body. It may also include information from the child and from you, as a parent. Information provided by the parent of another child would not form part of a child's educational record.

#### **As a parent, how can I access to my child's educational record?**

By making a request in writing to the Headteacher of the relevant academy.

#### **How long should this take?**

A request for an educational record must receive a response within 15 school days.

**How much will it cost?**

The academy can charge what it costs to supply a copy of the information. Full guidance on charging can be obtained from the Information Commissioners Office and the school may refer to that guidance on a case by case basis to ensure it is charging in accordance with the Regulations.

**As a parent, when can I request other information about my child?**

You will be able to access all the information about your child if your child is unable to act on their own behalf or gives their permission. As a general guide, a child of 12 or older is expected to be mature enough to make this kind of request.

**As a parent, are there circumstances where I could be denied access to my child's educational record?**

There are certain circumstances where the academy can withhold an educational record, for example, where the information might cause serious harm to the physical or mental health of the pupil or another individual.

**As a pupil, what rights do I have to access my information?**

You have (or someone acting on your behalf has) the right to a copy of your own information. This is known as the right of subject access. However, academies may withhold information in certain circumstances, such as where serious harm may be caused to your physical or mental health or another individual, or where the request is for an exam script or for exam marks before they are officially announced.

**What if the information you want involves information about another person?**

Information about another person may not always be available to you. Unless the other person gives their permission, or it is reasonable in the circumstances to provide the information without permission, the school will be entitled to withhold this information.

If you have any enquiries in relation to this policy, please contact:

Mrs Jennie Walker, Executive Principal, ACE MAT

Mr Stephen Gibson, Headteacher, Charlestown Primary School

Mrs Angela Jeffery, Headteacher, Gatehouse Academy

Mr Ewan Murray, Headteacher, Robartes Academy

Mrs Carol Wint, Headteacher, St Agnes Academy

Mr Antus Phillips, Headteacher, St Columb Major Academy

Mrs Nikki Cotterill, Associate Headteacher, St Columb Minor Academy

OR

The Business Manager, ACE MAT Business Team, c/o St Columb Minor Academy, Porthbean Road, Newquay, TR7 3JF

**ACCESS TO PERSONAL DATA REQUEST**

Surname		
Forenames		
Enquirer's Address		
Enquirer's Postcode		
Telephone Number		
Are you the person who is the subject of the records you are enquiring about		YES / NO
If NO, do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?	If YES, Name of child or children about whose personal data records you are enquiring	
Description of Concern / Area of Concern		
Description of Information or Topic(s) Requested (In your own words)		
Please send reply to	Please refer to Appendix 1	

**Data Subject Declaration**

I request that the academy search its records based on the information supplied above, under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the academy.

I agree that the reply period will commence when I have supplied sufficient information to enable the academy to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

**Signature of "Data Subject" (or Subject's Parent) .....**

**Name of "Data Subject" (or Subject's Parent) (PRINTED) .....**

**Dated .....**

**Authorised Officers**

Nominated person responsible for Data Protection and Freedom of information:

ACE MAT:	Neil Sampson, Business Manager, ACE MAT Jennie Walker, Executive Principal, ACE MAT
Charlestown:	Mr Stephen Gibson, Headteacher, Charlestown ACE Academy
Gatehouse:	Mrs Angela Jeffery, Headteacher, Gatehouse ACE Academy
Robartes:	Mr Ewan Murray, Headteacher, Robartes ACE Academy
St Agnes:	Mrs Carol Wint, Headteacher, St Agnes ACE Academy
St Columb Major:	Mr Antus Phillips, Headteacher, St Columb Major ACE Academy
St Columb Minor:	Mrs Nikki Cotterill, Associate Headteacher, St Columb Minor ACE Academy