Data Protection Policy

EBN Trust

Created:	**Sept 15**	
Reviewed:		
Ratified:		**Signed:**

Data Protection Policy

Introduction

EBN Academy Trust needs to keep certain information about its students, employees and other users. It is necessary to process this information so that courses can be organised, staff recruited and paid, and statutory obligations to funding bodies and other organisations complied with. To remain within the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the school must comply with the Data Principles that are set out in the Data Protection Act 1998. In summary, these state that personal data shall:

- be obtained, and processed, fairly and lawfully and shall not be processed unless certain conditions are met;
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose be adequate, relevant and not excessive in relation to the purpose for which they are held;
- be accurate and kept up to date;
- be kept no longer than is necessary for the purpose for which they are held;
- be processed in accordance with the data subject's rights;
- be kept safe from unauthorised access, accidental loss or destruction;
- not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

All staff, governors, students or others who process or use any personal information must ensure that they follow these principles at all times. It is intended that this Data Protection Policy will help to ensure that this happens.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies adopted by EBN Academy Trust from time to time. Any failure to follow the policy may therefore result in disciplinary proceedings.

Any member of staff or student who considers that the policy has not been followed in respect of their own personal data should raise the matter with the school Director of Finance and Resources in the first instance.

Notification of Data Held and Processed

All students, staff and other users are entitled to:

- know what information is held and processed about them within EBN Academy (Phase1 and 2) and why;
- know how to gain access to it;
- know how to keep it up to date;
- know what is being done within the EBN Academy (Phase 1 and 2) to comply with the obligations of the Data Protection Act.

Responsibilities of Staff

All staff will be provided annually with a data checking sheet. This will show all the types of data that are held and processed about them, and the reasons for which they are processed and provide the opportunity for staff to amend data if it has changed thereby allowing school records to be updated. All staff are responsible for:

- checking that information that they supply to EBN Academy (Phase1 and 2) in connection with their employment is accurate and up to date;
- informing the Business Manager of changes to information which they have provided, e.g. changes of address;
- checking the information which will be sent out from time to time, as detailed above;
- Informing the Business Manager of any errors or changes. EBN Academy (Phase1 and 2) cannot be held responsible for any errors unless notification of those errors has been received.

If and when as part of their responsibilities, staff collect information about other people (e.g. about students' coursework, opinions about their ability, references for students or other staff, or details of personal circumstances) they must comply with the guidelines for staff, which are at Appendix 1.

Data Security

All staff are responsible for ensuring that:

- any personal data which they hold are kept securely and not taken off site without the permission of their line manager;
- Personal information is not disclosed either orally or in writing, accidental or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or kept only on memory stick which is itself kept securely;
- Staff must report immediately, as part of the school's Whistle Blowing Policy, if they suspect that security of personal data has been compromised.

Parent /Carer and Student Obligations

Parents/Carers and students must ensure that all personal data provided to EBN Academy Trust is accurate and up to date. They must ensure that changes of address, etc are notified to the academy administration.

Rights to Access Information

Staff, students and other users of EBN Academy Trust have the right to access any personal data that is being kept about them either on computer or in manual files. Any person who wishes to exercise this right should make a written request to the school Business Manager or Principal in the first instance. Any other member of staff receiving a request for access to personal data **must** pass on that request to the Principal, who will ensure that the request is dealt with accordingly.

Where users are not either employees, students or members of the Governing Body, the request should be in writing and addressed to the Principal; there may well be a charge simply to cover the administrative

costs of extracting and photocopying the information on each occasion that access is requested. This charge can be waived at the discretion of the Business Manager.

EBN Academy Trust aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days, unless there is good reason for delay. In such cases, the delay will be explained in writing to the person making the request.

Publication of EBN Academy Trust Information

Information that is already in the public domain is exempt from the 1998 Act. It is the policy of EBN Academy Trust to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names of EBN Academy Trust Governors
- Names of Senior Leadership Team
- School Policies

Fair Processing Notice

EBN Academy Trust has a duty under the Children's Act and other enactments to ensure that staff are suitable for the job. The academies also have a duty of care to all staff and students and must therefore make sure that employees and those who use the academy facilities do not pose a threat or danger to other users. All adults, both staff and volunteers, will undergo a CRB check. The school will also ask for information about particular health needs. The academy will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

The Data Controller and Designated Data Controllers

EBN Academy Trust as a corporate organisation is the data controller under the Act, and the Governing Body is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day to-day matters.

The Academies' designated data controllers are the Business Manager for personnel data and Principal's PA for student and curriculum data. In the absence of the Business Manager, any issue needing urgent attention relating to the provisions of this policy should be raised with the Principal, or other member of the Senior Management Team acting on behalf of the Principal.

Retention of Data

EBN Academy Trust will keep some forms of information for longer than others. The retention of data is governed in many cases by legislation. For employees this includes information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. For students this includes information necessary for future references.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of EBN Academy Trust. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to academy facilities being withdrawn, or in the most serious cases, a criminal prosecution

Appendix 1 – Guidelines for Staff

Data Collection

You must ensure that you only collect data for the purposes for which the academy is registered. You should not create any data storage system (e.g. database, spreadsheet, computerised mailing list, or manual filing system) which holds personal data without the knowledge and permission of your line manager. Do not set up, or allow your staff to set up any of the above without with the Business Manager in the first instance. You must also notify the Business Manager of any new systems, or changes to existing systems for the processing of personal data, whether electronic or manual.

The Academy is registered to hold data for the following tasks:

1. Administrative Support - E-mail, security system, office administration
2. Personnel/Employee Administration - Recruitment, payroll, pension, employment related records
3. Purchase/Supplier Administration - Financial details, supplier records, orders, invoices etc.
4. Work Planning and Management - Rotas, project management, vehicle or equipment usage records
5. Public Relations and External Affairs - Promotion of links with external organisations and individuals
6. Marketing and Selling - Advertising, mail shots, promotional campaigns, canvassing
7. Lending and Hire Services - Leasing of materials or equipment, reservation/booking and recall systems
8. Research and Statistical Analysis - Research work, questionnaires, interviews, research analysis
9. Education and training administration - Student records, examination data, curriculum planning
10. Consultancy and Advisory Services - Consultancy, advisory services to employers (This register entry relates particularly but not exclusively to work with employers.
11. Fund-raising - Administration of appeals or other charity fund-raising initiatives If you are at all unsure as to whether what you want to do is covered, please contact the Business Manager or Headteacher.

Please also get in touch if you feel that there are areas of the academy's work that are not adequately covered.

Responsibility to Data Subjects

You must ensure that when you are asking for information, the supplier of that information knows what it will be used for. For example, if you are collecting data on a form, include a sentence or paragraph which explains the need for the information, and who will have access to it. If you are asking for sensitive data, you must make sure that the subject signs to give 'express consent' for those pieces of data to be collected. If you are unsure about whether the information is sensitive, consult the Business Manager.

If you are collecting data by interview, or over the telephone, again ensure that you make clear at the start of the interview that the person that you are talking to understands why you are asking for the information, and what it is to be used for.

Sufficiency

Collect only as much information as is necessary. Be very clear about the intended use of the data, and restrict the data collection to that information which will allow you to carry out that task. If it is possible to avoid the use of 'personal data', i.e. to work with data from which individuals *could not be identified*, then this should be done. Take every possible step to verify that the information that you are collecting is accurate. Where there are opportunities to check information, e.g. by cross-referencing with manual records

or by using tools within your software (spellcheckers, post-code verifiers) then take them. Your data should always be as accurate and up-to-date as possible. Ensure that you have routines to correct any inaccuracies that come to light as soon as they are spotted. It is poor practice to leave data errors uncorrected, and in certain circumstances, can be disastrous, an erroneous digit in a payroll record for example.

Currency

Regularly review the data that you hold, and make sure that information is as up-to-date as possible. If your use of the data is ongoing, build in routines which will allow people to update the information that you hold on them. This can be as straightforward as asking people to notify you of a change of address.

Reports and Analysis

Make sure that any data processing, i.e. production of reports or statistical analysis, is done accurately, and in such a way that will not change or distort your source data. Do not expect untrained staff to carry out complicated statistical tasks, and ensure that **only** those who are entitled to see the information are responsible for working with it.

Retention

Do not hold information for longer than is necessary. (Interview and recruitment data will be held for 1 year, Accounting Records for 6 years, Personal files for 7 years and student data for 3 years). The Academy Trust must be able to justify the storage of any data, at any time. In accordance with statutory regulations, and academy policy, archive where necessary, and delete data which is no longer of any use. DO NOT hold on to information just because you feel that it 'may come in useful' one day.

Disclosure

Only pass on information to those who are authorised to see or use it. Ensure that anyone from within the academy requesting data has a bona fide need for the information. If you are unsure as to whether you should disclose information internally, consult the Business Manager for advice. Never give information to an external enquirer without written proof of authorisation. Do not give details over the telephone, and ensure that your staff are aware of this restriction. If you believe that the enquirer has a legitimate right to receive information, and it is not practicable to delay disclosure, in the case for instance, of a police officer investigating an alleged criminal offence, please forward the query to the Business Manager or Principal. (The only exception to this is in the case of a genuine emergency, in which case information may be disclosed to the emergency services.) Any person, about whom information is held within a computerised or manual system in the Academy, has the right to see whatever information is being held, and to request that it be altered, should they regard it to be inaccurate. The academy complies with the Freedom of Information Act; anyone wanting to see their personal information should make a request in writing to the Business Manager in the first instance. Please refer anyone asking to see his or her data to the Business Manager.

Security

This is one of the most important aspects of data use, and the one to which all staff should pay close attention. Staff should ensure that where personal information is stored, care is taken wherever possible to restrict access to the data. It should not be possible for people walking in to an office, or walking past a computer screen, to read personal data. Similar care needs to be taken with the location and storage of printouts. Paper based systems containing personal data should be kept in locked drawers or filing cabinets. All unwanted data should be shredded and only carried out by staff who understand the importance of security in this context. Computerised systems containing personal data should be fully password protected, the passwords changed regularly, and individuals made aware of the necessity to

maintain the secrecy of their personal passwords. Passwords must never be given to students or unauthorised staff. Users should make sure that unauthorised personnel are not able to read personal data from their computer screens.
Users of the network should use only their own login passwords, in order to maintain the security of the network system, and enable an 'audit trail', should the network's security be compromised. Computers that are not in use should be logged out or switched off. Offices containing computers should be kept locked when not in use. Back-ups of data should be regularly carried out, and the back-up media held securely. Unwanted printouts or other files containing personal data should be shredded.

Personal data should be disclosed only to authorised personnel. The long-term storage of Academy-related personal data off-site is subject to the prior approval of the Business Manager. Staff working on personal data at home should be aware of the security required for such data, and should ensure that unauthorised access is not given. Academy software and hardware should not be removed from academy premises without prior authorisation. Any perceived breaches of the security of personal data held by the school should be reported immediately to the Business Manager

Appendix 2 – Glossary of Terms

The Act - The Data Protection Act 1998

Data - Any information that will be processed or used within or by a computerised or manual system. This can be written, taped, photographic or other information.

Data Subject - The person to whom the data relates.

Data Controller - The person or organisation responsible for ensuring that the requirements of the Data Protection Act are complied with.

Designated Data Controller - Individual appointed by the Academy Trust to carry out the day-to-day duties of the Data Controller.

Manual System - Any paper filing system or other manual filing system which is readily structured so that information about an individual is readily accessible.

Personal Data - Information about a living person that by itself, or in conjunction with other information which is kept in a manual or computerized system, is sufficient to identify an individual. This information is protected by The Act.

Processing - Accessing, altering, and adding to, changing, disclosing or merging any data will be processing for the purpose of the 1998 Act.

Sensitive Data - Information about a person's religion or creed, gender, trade union membership, political beliefs, sexuality, health or criminal record.

Subject Consent - Before processing personal data, the Academy Trust must have the agreement of the individual to do so. In the case of sensitive data, this must be specific consent, but in other cases, it can be more general.

The Data Protection principles - the underlying principles of the Act that determine what data can be collected, processed and stored. A failure to abide by the principles will be a breach of the 1998 Act.

The Data Protection Commissioner - Person Appointed by the government to administer the provisions of the 1998 Act including notification and to provide guidance and assistance to organisations and individuals.

The Data Protection Tribunal - The tribunal established to deal specifically with matters of enforcement under the Data Protection Act.

Signed Chair of the Governing Body: _____Date:_____