EAST BARNET SCHOOL

"I want to learn"

INFORMATION POLICY

(Incorporating Data Protection)

Version 2.0

Review by Chairs & Vice-Chairs Committee:	23rd May 2016
Adopted by Governing Body:	20th February 2017
Next Full Review Due:	Spring 2019
Reviewer:	L. Swaine
Governor Link:	Chair of Governors

INFORMATION POLICY (inc DATA PROTECTION)

East Barnet School, Chestnut Grove, East Barnet, EN4 8PU

A. Statement of Principle

East Barnet School recognises through its Information Policy the rights of access and confidentiality surrounding all personal information held by the school and information held about the school. It adheres to the Data Protection Principles as laid out in the London Borough of Barnet's guidance and in doing so upholds the **Data Protection Act (1998)** and the **Freedom of Information Act (2000).**

Governors, Senior Leaders and Staff take all reasonable steps to meet their responsibilities and to promote good practice in the handling and use of personal information.

The School, including its clubs, societies and PTA, will take action to make sure the personal information it handles is protected. It will ensure there are adequate checks in place to confirm that policies and procedures concerning the secure use of personal information are working correctly.

B. The Eight Guiding Principles

The School by its very nature contains within it a number of "Areas of Operation". Each Area of Operation may apply the eight principles using a different procedure or system dependent upon the nature of its responsibilities. However, regardless of each "Area of Operation's" function, its structure or location, the Eight Principles all apply.

A definition of data and other terms is contained in appendix 1.

- **First Principle**
  Personal data will be lawfully and fairly processed in accordance with the **Data Protection Act 1998** and the **Freedom of Information Act 2000**.

- **Second Principle**
  The School will hold the minimum personal data necessary to enable it to perform its legitimate interests and activities.

- **Third Principle**
  Every effort will be made to ensure that information is accurate and up to date and that inaccuracies are corrected without unnecessary delay.

- **Fourth Principle**
  Personal data will be accurate in respect of matters of fact. Opinions will be carefully and professionally expressed.

- **Fifth Principle**
  Personal data shall not be kept for longer than is necessary for the purpose which it was produced. A regular review should be conducted.

- **Sixth Principle**
  When appropriate, the School will respond to and comply with requests for access to relevant personal/professional data from stakeholders and, where necessary, professional agencies.

- **Seventh Principle**
  Personal data will be kept in an appropriately controlled and secure environment.

- **Eighth Principle**
  Data will only be transferred to other schools/institutions/professional agencies based on strict Data Protection guidance.

C. The Rights of Members of the Public

Members of the public have extensive rights to access data and information held by the school. These are laid out in the school's 'Publication Scheme for Information Available Under the Freedom of Information Act 2000' and are summarised below:

1. anyone can request information and data (on computer and/or paper) that the school (The Data Controller) holds about them, or about the school in general;
2. an individual is entitled only to their own personal data, and not to information relating to other people;
3. the request must be made in writing and is called a 'Data Subject Access Request';
4. all written requests for copies of personal data must be complied with within 40 calendar days;
5. reasons for refusal of a request or withholding of information must be given to the applicant.

Note: The school has the right to charge for access to personal data and the current fee is £10 per request. (There is no charge for students, pensioners, benefit claimants and those on Income Support.)

D. Exemptions

Generally, the school is exempt from its duty to disclose under the Act in certain circumstances. However, it does not exempt the school from ensuring that the data is processed in accordance with the Data Protection principles. The main exemptions relating to disclosure of data held by East Barnet School are as follows:

1. where personal data relates to another person (data subject). In this situation, the consent of the other data subject will also be required in writing. A child over the age of 12 is deemed to be able to make their own request, or must give written permission if a parent makes the request;
2. where the information is already publicly available;
3. the examination marks and personal data contained in examination scripts;
4. where the personal data consists of educational records or relates to social work;
5. where the personal data relates to adoption records and reports, statements of a child's special educational needs and parental order records and reports;
6. in the case of health records, where it could result in serious harm to the physical or mental condition of the data subject or another person;

7. where it would not be in the interests of prevention or detection of crime, apprehension or prosecution of offenders.

E. Requirements

The School, as overall Data Controller, will register annually with the Information Commissioner (who maintains a public register of the type of information processed by organisations, where it is obtained from and the purposes for which it is used).

The Headteacher is the current designated Data Protection Compliance Officer.

Where the school or a member of staff receives a phone call requesting personal or sensitive information, the following action must be taken:

a. If the caller does not mention FOI - then it should be dealt with as deemed appropriate - which might be to refuse, depending on the nature of the request;
b. If the caller says it is an FOI Request - it should be explained that this must be sent in writing and they should be given the school address or email to which it should be sent.

Guidance and full details about the Data Protection Act are available from the Information Commissioner's website (www.ico.gov.uk). The section describing the current rules on right of access should be checked before granting or declining an FOI request.

F. Staff Responsibilities

Listed below are some of the key responsibilities under the Data Protection Act 1998. The main issues are equally relevant to Governors and PTA Officers. Guidance and advice for carrying out these responsibilities and requirements can be found in the Appendices.

1. Everyone has a personal responsibility to ensure that any personal data they process complies with the data protection principles; that they adhere to the school's professional expectations; and comply with the AUP (Acceptable Use Policy) to which they are a signatory.
2. Data Controllers must ensure that their area of operation complies with the Act and their use of personal data is registered. Data Controllers must also ensure that relevant staff remain aware of the appropriate procedures.
3. All staff managing and handling personal information must be regularly and appropriately trained to know what to do.
4. The authorisation of a member of the Senior Leadership Team is necessary before any employee uses their own computer at home to access or process data belonging to the school or takes data out of the workplace for processing on a computer owned by the school.
5. Staff should take all possible measures to ensure all data accessed, processed or stored is kept secure.
6. Staff can only pass on information to any other organisation by observing the school's formal procedures and Acceptable Use Policy. If in doubt then the guidance of a member of the Senior Leadership Team must be sought before any information leaves the school.
7. Any member of staff knowingly or recklessly breaching the school's Information Policy may be subject to the established disciplinary procedures.

8. Where the school receives a complaint about, or is alerted to, a potential breach of Data Protection, it will carry out an investigation in line with the school's Complaints Procedure.

G. Areas of Operation

The School's Areas of Operation are listed below and have individual procedures and systems which support this Information Policy. The procedures and practices adopted by the Areas of Operation are subject to regular review.

1. Finance complies with AFMG *(Academies Financial Management and Governance)* procedures
2. Information Technology follows AUP *(Acceptable Use Policy)*
3. Staff Personal Data
4. Staff Professional Data
5. Student Information (including Child Protection)
6. CMIS Data

Partially covered by AUP; all hard copies of data/information are kept in staff files and stored securely as outlined in appendix 2

Appendix 1

Definitions

1. **Personal Data**: Information held on a relevant filing system, accessible record or computerised record (as well as digital, audio or video equipment) which directly or indirectly identifies living individuals;
2. **Sensitive Personal Data**: Personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, criminal activities;
3. **Relevant Filing System**: A set of records which is organised by reference to the individual and is structured to make information readily accessible e.g. personnel records;
4. **Data Subject**: An individual who is the subject of the personal data, for example, a student;
5. **Processing**: This includes recording or holding data, organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying of data.

Appendix 2

Data Protection Guidance for Staff and Governors

Key points

1. The Headteacher is the designated Data Protection Officer and first point of contact regarding compliance and enquiries.
2. Make sure you have read, understood and signed the school's Acceptable Use Policy (AUP).
3. You should be aware of your responsibilities to Data Protection and adhere to the school guidelines on the use of personal or sensitive information at all times. (See this policy and AUP for more details.)

As set out in the AUP and e-Safety Policy:

1. Where it is necessary for staff to electronically store personal information (that would cause damage or distress if it were lost or stolen), it must be located in the encrypted "Safe Store folder" as directed by EBS ICT Support.
2. Staff and Governors should not use laptops to store sensitive personal information, except where absolutely essential and under the guidance of the Data Protection Act 1998 and School Data Protection Policy. All personal data MUST be encrypted.
3. Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses.
4. Memory sticks or portable storage must be encrypted if used for storing the following types of data (especially if the data has to leave the school building): Confidential data, personal data, sensitive personal data, contract information, student, parent or staff Information, job applicant Information, business information.

Reminder list of some easy steps to take to keep information secure:

a. Clear desk policy - leave nothing on your desk that contains any personal or confidential data - even at home.
b. Be very careful about portable devices - do you need to take data outside of the school? Are there any processes you need to follow to do this?
c. Always think twice before doing any work (reading or writing using paper as well as laptops and other electronic equipment) in a public place - tube, bus, pub, etc.
d. Apply both physical and logical security when you work from home - keep work items (paperwork, CD-ROMs, memory sticks, etc.) secured as you would in school - and out of reach of anyone else.
e. Don't click on any links in emails from people you don't know. Always take great care clicking on anything in an email, even if you know the sender.
f. If you have emailed several people called, e.g. "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right one before sending.
g. If you want to send an email to someone without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see all the addresses it was sent to.

h. If you forward an email to someone, delete any email addresses which may appear in the body of the email.
i. Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
j. Only send emails to necessary people.
k. Keep distribution lists up to date - immediately remove names and addresses of people who have left or are no longer involved.
l. Ensure you lock your computer when you leave your desk using a password protected screensaver.
m. Never write your password on post-it notes or anywhere that people may find it.
n. Don't give your passwords to anyone.
o. Lock cabinets containing confidential data very night and during the day when you're not using them.
p. Shred sensitive data.
q. Keep your voice down if you have to have confidential conversations or make phone calls in public places, e.g. coffee shops, buses, corridors, staff room etc.
r. Check the print queue is actually going to the printer you think it is (send a test page or document first if unsure).
s. Use private print job function for sensitive data. Only print when absolutely necessary. Ask for instructions if you don't know how to do this.

Further guidance and details about Data Protection are available from the Information Commissioner's website (www.ico.gov.uk).

Appendix 3

Data Protection Guidance for PTA, Clubs and Societies.

EBS Clubs, Societies and PTA (hereafter referred to as 'Association') all fall under the control of East Barnet School as Data Controller. The school has an Information Policy which should be followed. It is available on the school website or as paper copy from the school office.

Please note that the Data Protection Act (1998) contains important requirements about the way in which personal data (i.e. information about living people) must be handled and subjects' rights to inspect and challenge the data. This includes information in electronic and paper form.

The Association is responsible for the handling of its own data. You will therefore need to think about the kinds of personal information held about the Association's committee members, as well as others who are on mailing-lists but who are not on the committee, and how this information is used. For example, if you photocopy a handwritten membership list and give out name-and-address details to external companies or to other schools if you are arranging joint events, you may be breaking the law.

The school's Headteacher is the designated Data Protection Controller and first point of contact for guidance or if a request for information is received.

Requirements

1. **Personal data must not be held without consent or unless absolutely necessary to fulfil a contract with the subject or to meet legal requirements, and then must be processed fairly and lawfully:** so it is OK for you to keep members' names on a written or electronic register and use this for the purposes of administering the Association (collecting donations, sending out minutes, organising elections, events etc) provided individual members agree to this.
2. **Personal data must be obtained for one or more lawful purposes and must not be further processed in any manner incompatible with the purpose(s):** so it is <u>not</u> OK for you to use the membership list to generate mailing-lists for use by external parties (e.g. sponsors, other organisations) unless individual members specifically agree to this.
3. **Personal data must be adequate and not excessive for the purpose(s) for which they are processed:** so if you are asking members to provide details of home addresses, phone numbers, etc you need to consider whether such data is necessary for the purposes of the Association's activities.
4. **Personal data must be accurate and where necessary kept up to date.**
5. **Personal data must not be kept for longer than necessary for the purpose(s) originally collected;** so you need to be careful about retaining details of members who are no longer part of the Association – the Association might want them for its historical records, but must not use such information as the basis of mailshots (e.g. for fund-raising) unless the subjects consented to that when the data was originally collected.
6. **Personal data must be processed in accordance with subjects' rights under the Act: these include the subject's right to inspect the data held about him or her (but not data about other people);** to prevent the processing of data; to correct, block or erase data; to sue for damage

caused; you need to bear in mind that the Association collectively, or individual officers, could be prosecuted for breaches of the Act.

7. **Appropriate technical and organisational measures must be taken to prevent unauthorised/unlawful processing of personal data and against accidental loss, destruction, damage**; so if the Association is holding its data on computer, you need to be careful about who is able to access and process the data; all personal data should be encrypted, especially if stored on laptops, pen drives or other portable devices. Even if the records are paper-based, they must be kept secure.
8. **Personal data must not be transferred, without the subject's consent, outside the European Economic Area unless the country concerned ensures an adequate level of protection for the rights and freedoms of data subjects;** this needs to be borne in mind if a member takes Association records out of the UK (e.g. on a laptop computer while on an exchange visit, sporting event or away on business).
9. **When people become Association members, or renew their subscriptions, it is important to make clear to them what personal data will be held and what use the Association wants to make of this;** this should be done as a 'tick box' on the form that a member fills in with their name and contact details when they join. Please bear in mind that data-subjects can withdraw their consent for particular uses at any time.
10. **The Association will need to keep under review what personal data is held; where and how securely held; and what the data is being used for.**
11. **The Association's mailing-list should NOT be used to circulate information from or to third parties;** (e.g. companies advertising special deals for school equipment), unless the Chair, Secretary or whoever is controlling the mailing-list is absolutely sure that the information is directly relevant to recipients and that those in the list have expressed an interest in receiving that kind of information. Under no circumstances should the Association's membership register or mailing-list be given to third parties. Otherwise, the Association will potentially be in breach of the Data Protection Act.