Fairstead House

DATA PROTECTION POLICY INCLUDING RISK ASSESSMENT
Incorporating the Early Years Foundation Stage

INTRODUCTION

Fairstead House School recognises and accepts it responsibility as set out in the **Data Protection Act 1998 and Freedom of Information Act 2000** and sub-legislation contained therein. The School will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information held in manually and electronically in the organization. In particular the School will comply with the Data Protection Principles set out in the 1998 Act 1998 and Freedom of Information Act 2000.

This policy statement applies to all School Governors and employees, and individuals about whom the School processes personal information, as well as other partners and companies with which the School undertakes it business.

SCOPE

The School needs to collect and use certain types of personal information about people with whom it deals in order to operate. These include current, past and prospective employees, pupils, suppliers, clients, and others with whom it communicates. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used - whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Data Protection Act 1998 and Freedom of Information Act 2000.

We regard the lawful and correct treatment of personal information by the School as very important in order to secure the successful carrying out of operations and the delivery of our services, and to maintaining confidence with those whom we deal. The School wishes to ensure that it treats personal information lawfully, correctly and in compliance with the 1998 Act and Freedom of Information Act 2000.

To this end we fully endorse the obligations of the Act and adhere to the Principles of data protection, as enumerated in the 1998 and 2000 Act. The nominated data controller is Fairstead House School.

RELEVANT DATA

For data protection purposes, "personal data" includes all information in education records, including names, dates of birth, addresses, school marks, medical information, exam results, and SEN assessments. Information relating to race and ethnicity, political opinions, religious beliefs, physical or mental health, sexuality and criminal offences is "sensitive" personal data and particular care must be taken in storing and processing such data.

ROLE OF THE DATA CONTROLLER

(a) The Data Controller must notify the processing of personal data with the Information Commissioners Office. The School must supply certain information to the Commissioner who maintains a public register of the types of information organisations process, where it gets it from and what it does with it.

(b) Observing the eight Data Protection Principles (more detail below).

(c) Allowing the data subject to exercise his/her rights and have right of access to their personal information, what is held, how it is processed, to whom it is disclosed and to be told of the logic behind automated decisions. Such access requests must be complied within 40 days and a fee can be applied.

DEFINITIONS

Data Controller Any individual or organisation who controls personal data, in this instance the School.

Personal Data: Information held on a relevant filing system, accessible record or computerized record (as well as digital audio or video equipment), which identifies living individuals.

Sensitive Personal Data: Personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life and criminal activities.

Relevant Filing System: Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a say as to make specific information readily accessible e.g. personnel records, microfiches.

Data Subject: An individual who is the subject of the personal data, for example, employees, pupils, claimants etc.

Processing: Obtaining, recording or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.

Accessible Records Any records which are kept by the Organisation as part of a statutory duty, eg pupil records, housing tenancy records, social services records.

DATA PROTECTION PRINCIPLES

Specifically, the Principles require that personal information:

1. shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions as set out in the 1998 Act are met;
2. shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4. shall be accurate and, where necessary, kept up to date;
5. shall not be kept for longer than is necessary for that purpose or those purposes;
6. shall be processed in accordance with the rights of the data subject under the 1998 Act and Freedom of Information Act 2000.

and that:

7. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
8. shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

COMMITMENT

The School will, through appropriate management and application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used, including its accuracy and relevancy for the purpose(s) specified;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the 1998 Act and Freedom of Information Act 2000. (These include: the right to be informed that processing is being undertaken: the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, block or erase information which is regarded as erroneous);

- take appropriate technical and organisational security measures to safeguard personal information; and
- ensure that personal information is not transferred abroad without suitable safeguards.

COMPLIANCE

In addition, the School takes steps to ensure that:

- there is someone with specific responsibility for data protection in the organisation. (Currently, the nominated person is the Head);
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so and supervised;
- anybody wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are clearly described;
- a regular review and audit is made of the way personal information is managed;
- methods of handling personal information are regularly assessed and evaluated;
- performance of handling personal information is regularly assessed and evaluated; and
- it disseminates to employees, information on good practice in respect of handling, using and storing personal information.

All employees of Fairstead House School will be made aware of this and any subsequent changes to this policy statement through the usual process. The policy and practice will be reviewed annually, added to, or modified from time to time and may be supplemented in appropriate cases by further statements and procedures relating to the work of the particular groups of workers.

Attachment: Risk Assessment for Data Protection and Information Security

Specific to the Early Years Foundation Stage

Documentation: "Providers must maintain records, policies and procedures required for the safe and efficient management of the settings and to meet the needs of the children."

- Providers must keep the following information:
  - Name, home address and telephone number of everyone employed on the premises.

- Name, home address and telephone number of anyone else who will regularly be in unsupervised contact with children in the EYFS.

- A daily record of the names of children looked after on the premises, their hours of attendance and the names of their key workers.

- A record of the risk assessment clearly stating when it was carried out, by whom, the date of review and any action taken following a review or incident".

- These records are kept in a centrally accessible area (the School Office and the Bursar's office for the documentation and the risk assessments on the school server or in the classrooms or Bursar's office depending on the type).

- Parents are always informed of an impending inspection.
- We ensure that all parents and carers are given copies of inspection reports as soon as they are made available.
- Records relating to individual children are retained until the child reaches 25 years of age (or if pupil is not admitted to the school for 7 years after that decision.
- We store our data in secure areas and records on staff and children are only accessible to those who have a right or professional need to see them.
- All staff are made aware of the need for confidentiality.

DATA ENCRYPTION

To reduce the risk of loss of data or unauthorised access to data held by the school on portable devices Fairstead House School has established a policy of data encryption. This covers data which can be accessed from outside the school and which can be removed from the school.

This policy covers data stored by the following means:

- Portable storage devices such as USB data sticks, external drives
- Removable media such as DVDs, CDs, floppy disks etc

IMPLEMENTATION

Portable storage devices such as USB data sticks must be encrypted before use with individual passwords in order that their portability is maintained. Fairstead House School prohibits the use of non-encrypted data storage devices at all times.

The school recommends the Kingston Secure or Integral Secure encrypted USB sticks.

Any data from a USB data stick used elsewhere must be resaved onto the stick and permanently deleted from any other system, machine or device.

Removable media such as CDs and DVDs must also be encrypted and will prompt the user to enter a password before they can be used.

Users will not remove or copy sensitive or personal data from Fairstead House School's premises unless the data storage device is encrypted and is transported securely for storage in a secure location.

Users must not publish any documents containing personal data on externally accessible websites.

The encryption process will be managed by the school's ICT Coordinator. Passwords must be kept confidential by users and must be complex (eg 8 characters including a capital and a number). Passwords must be changed at least annually.

All incidents resulting in a breach of these guidelines must be reported to the Head.

As required by ICO regulations, the Head will inform the Information Commissioner's Office (ICO) if there are any losses of personal data.

DISPOSAL OF RECORDS and DESTRUCTION OF DATA

The Data Protection Act 1998 states that personal data must not be kept for any longer than is "*reasonably necessary for its particular purpose*".
This means that with any document or written record, the starting point must be to analyse its: (1) particular use; (2) content; and (3) importance. However, even after that, you cannot just shred it!

The law sets strict 'limitation periods' on when a company's various legal obligations expire. So once you have considered the above you will also need to categorise the document e.g. is it contractual, employment, tax, health and safety or business-related?

If a record is disposed of before its applicable limitation period ends, there is a real risk that the School will have difficulty defending any criminal or civil proceedings brought against it or the Board of Governors.

Whilst there are statutory limitation periods, documents should be kept securely in locked cabinets and the following minimum retention periods apply for both paper and electronic records:

1. **Fairstead House School business documents** - paperwork relating to the running of the business e.g. minutes of Governors' sub-committee meetings, Senior Management Team meetings, contracts and service agreements should be kept for at **least ten years**.

   The minutes of Governors meetings are kept **indefinitely**.

   Responsibility: Bursar **Storage:** Locked cupboard in office or attic

2. **Tax and accounting records** - retain for **six years** from the end of the accounting period they refer to.

   Responsibility: Bursar **Storage:** Locked cupboard in office or attic

3. **Personnel documents** Retain for a minimum of seven years from the end of employment.

   Pension records Permanent

   Job application interview/rejection Minimum 3 years

   Responsibility: Bursar **Storage:** Locked cupboard in office or attic

4. **DBS Certificates** No longer than 6 months

   Responsibility: Bursar **Storage:** Locked cupboard in office

5. **Health and safety records** - documents such as accident books and records of reportable injuries must be kept permanently.

   Risk assessments 7 years from completion of activity.

   Responsibility for staff H&S records: Head **Responsibility for pupil H&S records**: Head

   Storage: Locked cupboard in Head's office

6. **Former Pupil records** - documents such as pupil files and pupil sanctions records should be kept securely until the pupil has reached the age of 25, when they will be destroyed. They will not be disclosed to any third party, unless required by statutory regulations. Examples of pupils' work and less sensitive data should be destroyed after the child leaves the school.

   Special Educational Needs Until pupil is 35 years of age

   Incident reporting Keep on record for 35 years

   Responsibility for Former Pupil files: Head **Responsibility for Former Pupils' work**: Class teacher with Head's agreement

   Storage: Locked attic

7. **Old registers** – should be kept for 6 years after the last entry and then archive.

   Responsibility for Registers: Head **Storage:** Locked attic

Disposal of records should be by secure method such as shredding or burning and, in the case of electronic records, secure destruction.

Fairstead House

DATA PROTECTION RISK ASSESSMENT
This is a generic risk assessment that identifies the common hazards and risks associated with Data Protection and Information Security. It has been assessed as part of a whole School Health and Safety audit and will be regularly reviewed and updated.
Staff are aware of the risk assessment and will consult it regularly.

The school's IT coordinators are Michael Redford and Debra Meyer
The school's IT Consultant is Ian Braybrooke of TBM Ltd 01638 665240 ian.@tbmuk.com

Assessment Date: 10/02/2016 Assessed by :VP Checked by: LB/MR

Hazards H/M/L risk?		Who might be harmed?	Is the risk adequately controlled?	What further actions are needed to control the risk?	Tick if in Place	Outcome H/M/L risk
Loss of data from computers in School	H	School's reputation Families Staff Financial viability	• All computers and laptops in school have up-to-date anti-virus software • all computers and laptops are username and password protected • passwords are complex (8 digits including a number and a capital eg Teach1ng) • screen saver should come on after no more than 5 minutes • screen savers password protected • staff to access only data relevant to them on a need-to-know basis • passwords not shared • passwords not written down or e-mailed to anyone • server areas password protected (MR and Ian Braybrooke of TBM Ltd have access) • passwords changed termly • remote access not allowed without Head/Bursar's agreement • computers switched off when staff not in the building • firewalls and anti-virus systems on all computers • system "lock-downs" to ensure corrupt data cannot be uploaded • mobile phones and i-pads should not be used	All staff to check screen savers		H

	M		for sensitive data unless permission of the Head is given.			
Access to unauthorized data in school	M	School's reputation Families Staff	• Information on server is setup so that each member of staff or pupils only have access to their authorised areas			M
Data kept unnecessarily	M	School's reputation Families Staff	• Data processed fairly and not unnecessarily • Data used only for purposes for which it was not intended and must be adequate and relevant			M
Data kept longer than necessary	H	School's reputation Families Staff	• Good housekeeping – data checked, updated and deleted at least annually • Former Pupil files stored in the locked attic and destroyed by secure destruction when pupil reaches 25 years • Staff files kept stored in the locked attic and kept for 7 years • Business documents destroyed after 6 years.	All staff to implement		L
Loss of computers through theft, arson or other event	H	School's reputation Families Staff Financial viability	• Computers are password protected • Hard discs should be encrypted • Password protected screen servers should be used where appropriate • Rooms with computers with data stored on them should be locked when not in use • Buildings are locked and alarmed when not in use • Only key individuals have access to codes and alarm systems • Visitors should report to the office and wear a badge when on site • Data is backed up nightly from the Server, through TBM Ltd in the "cloud" through Avecoh.co.uk (Tier 3 Specified, back-up in Iceland) to meet legislative requirements.	For Head, Bursar, Office staff and teaching staff as appropriate		H
Loss of stored data on file, disc or memory stick in School	**H**	School's reputation Families Staff Financial viability	• Any filing cabinets containing sensitive data should be locked when not in use • Rooms containing sensitive data should be locked when not in use • Keys should be stored securely in the locked cabinet • The key to the cabinet should be kept separately and GW Has a spare			H

			• Memory sticks containing sensitive data should be encrypted and stored safely. Eg "Kingston Secure" or "Integral Secure" • The server is backed up nightly so there should be no need for further back-ups. Any other back-ups should be encrypted • The remote back-ups are stored in the EU or Iceland			
Loss of stored data on file, disc or memory stick out of School	H	School's reputation Families Staff Financial viability	• Sensitive data should not be stored on laptops or on home computers without permission from the Head/Bursar • Sensitive data should be deleted from laptops or home computers as soon as possible after it has been used unless the data is encrypted • Any laptop or memory stick should be protected from unauthorised access by encryption • Any laptop or memory stick should be protected from unauthorised access by physical security eg a laptop should not be left in a car where it can be seen and should not be left in the car if the vehicle will be unattended for some hours.	Staff as appropriate		H
Inadequate destruction of data	H	School's reputation Families Staff Financial viability	• Any sensitive information on paper should be destroyed by shredding or burning • Memory stores no longer needed should be wiped then physically destroyed • Computers no longer required should be sent immediately to have their hard discs destroyed			H
Loss of data in transition	H	School's reputation Families Staff Financial viability	• E-mail and the internet are not secure unless authorised sites such as HMRC • Fax, post or e-mail may be intercepted or sent to the wrong person – care should be taken with sensitive data using additional security such as encryption or courier services if the data in sensitive • Sensitive data for the Early Years Funding should be sent to Suffolk CC by encrypted method			H

Lack of response to a breach of security	M	School's reputation Families Staff Financial viability	• Any breach of security must be reported to the Head or Bursar • The Head will report any loss of data to the ICO • An investigation will be carried out and the Governors informed • Appropriate action will be taken to contain and limit the extent of the exposure • Appropriate action will be taken to contain and limit the extent of the damage to the reputation of the School and any individuals affected • Disciplinary procedures may be instigated			H

Responsible: SMT
Date approved: Spring 2011
Reviewed: Spring 2016
Review Date: Summer 2017