Caring for young minds

The Family School London

An Anna Freud Centre Initiative

THE DATA PROTECTION POLICY

Date Approved by Governors	8 September 2016
Review Date	September 2017
Coordinator	HT
Principal Signature	Stephen Taylor

At the heart of all policies at The Family School are the following principles:

- Every young person in our school, whatever his or her personal circumstances can learn and achieve.
- Every young person in our school, whatever his or her self-perception and previous experiences, has academic and creative potential to become a valuable member of society.
- The key to learning at The Family School lies within the quality of the relationships between pupils, family members, staff and the intermediate agencies with whom we work.
- The success of our school is based on high expectations, mutual trust, caring for each other and taking responsibility.
- Every young person in our school is capable of becoming an agent for change in his or her local community.

Our vision is to provide our pupils with the confidence, academic progress, and ambition to take the next steps towards a successful and productive life and to be able to contribute positively within their local community and wider society.

Rationale:

This document is a statement of the aims and principles of the School for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

The Family School London needs to keep certain information about its employees, pupils and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

The information security objective is to ensure that The Family School's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any person unlawfully. To do this, The Family School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). 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 for that purpose;
- Be accurate and kept up to date;
- Not be kept for longer than is necessary for that purpose;
- Be processed in accordance with that data subject's rights under the Data Protection Act 1998;
- Be kept safe from unauthorised access, accidental loss or destruction
- 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

The Family School and all staff or others who process or use personal information must ensure that they follow these principles at all times. This means that they will:

- Explain for what purposes we will use information when we collect it
- Explain why, with whom and under what circumstances we will share information and assure confidentiality of personal or sensitive information
- Share personal information with others only when it is necessary and legally appropriate to do so, and set out clear procedures for responding to requests for access to personal information
- Check the quality and accuracy of the information we hold
- Apply our records management policies and procedures to ensure that information is not held longer than necessary
- Ensure that when information is authorised for disposal it is done appropriately and securely
- Ensure appropriate security measures to safeguard personal information whether that is held in paper files or on our computer system
- Ensure that information security training is available to all relevant staff
- Ensure that appropriate monitoring and reporting processes are put in place to identify and act upon breaches of information security.

Status of this policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controller

The Family School as a body corporate is the Data Controller under the 1998 Act and the governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters. The Designated Data Controllers are: Stephen Taylor, school Principal and Dianna Tzioras – Administrator

Any member of staff, parent/carer or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Designated Data Controllers

Responsibilities

The Family School Principal has direct responsibility for maintaining this policy and providing advice and guidance on its implementation.

All staff are responsible for policy implementation and for ensuring that staff they manage adhere to the standards. They are responsible for:

- Checking that any information that they provide to the school in connection with their employment is accurate and up to date
- Informing the school of any changes to information that they have provided, eg change of address, either at the time of appointment or subsequently. The school cannot be held responsible for any errors unless the staff member has informed the school of such changes.

If and when, as part of their responsibilities, staff collect information about other people (eg bout a pupil's work, opinion about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Data Protection Policy.

Subject Consent

In many cases, the school can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be obtained. Agreement to the school processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The school has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job.

The school has a duty of care to all staff and students and must therefore make sure that employees and those who use school facilities do not pose a threat or danger to other users

The school may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical conditions such as asthma or diabetes. The school will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person’s religion, health, criminal convictions, or race. This may be to ensure that the school is a safe place for everyone, or to operate other school policies such as the Sick Pay Policy or the Equalities Policy.

Because this information is considered **sensitive** under the 1998 Act, staff, parent/carers (and pupils where appropriate) will be asked to give their express consent for the school to process this data. An offer of employment or a parent/carer attendance on the Parent/Carer & Multi-family Programmes may be withdrawn if an individual refuses to consent to this without good reason. Due to the particular nature of The Family School, specifically its method of involvement of parent/carers in the daily work of the school, parent/carers are included in this section. A specific policy, the ‘Parent/Carer Induction Policy’ and its associated consent forms describe the requirements in more detail and should be read in conjunction with this policy. Parents/carers are asked to give consent when their child takes up a place at The Family School.

Publication of School Information

Certain items of information relating to school staff will be made available via searchable directories on the public website, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the school.

Retention of data

The school has a duty to retain some staff and student personal data for a period of time following their departure from the school, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Rights to Access Information

This policy should be read in conjunction with the Access to Pupils Records Policy in relation to handling requests for information.

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely
- Personal information is not disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party
- Information or data about pupils is shared with other staff as appropriate using the school’s secure email provider

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

Supporting Framework

In order to comply with the policy, The Family School will develop and maintain information security standards. Examples of measures to achieve this are physical security, virus control and the use of passwords for access control. The development of any new system will include information security analysis and requirements as part of the initial specification.

Implementation

This policy will be made available to all parents, guardians, staff (whether permanent or temporary) and governors.

General Security, storage and disposal of information

General Security

It is important that unauthorised people are not permitted access to The Family School information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access.

- Do not reveal pin numbers or building entry codes to people that you do not know or who cannot prove themselves to be employees.
- If you don't know who someone is and they are not wearing some form of identification, ask them why they are in the building (see safeguarding policy and sign – in procedure).
- Do not position screens on reception desks where they could be seen by members of the public
- Do not be afraid to challenge people who you do not recognise if they are not wearing an identity badge
- Lock secure areas when you are not in the office
- Beware of people tailgating you into the building or through a security door
- Do not let anyone remove equipment or records unless you are certain who they are.

Visitors and contractors in School buildings should always sign in a Visitors' Book.

Security of Paper Records

Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.

- Records that contain personal data, particularly if the information is sensitive, should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office.
- Always keep track of files and who has them
- Do not leave files out where others may find them.
- Where a file contains confidential or sensitive information, do not give it to someone else to look after.

Paper records should be disposed of with care. If papers contain confidential or sensitive information shred them before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.

Electronic software

- Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information.

- Keep suppliers' DVDs containing software safe and locked away. Always label the DVDs so you do not lose them in case they need to be re-loaded.
- When we buy a license for software, it usually only covers a certain number of machines. Make sure that you do not exceed this number as you will be breaking the terms of the contract.

Guidance for your password to the school IT network is:

- Don't write it down
- Don't give anyone your password.
- Your password should be at least 6 characters
- The essential rules your password is something that you can remember but not anything obvious (such as *password*) or anything that people could guess easily such as your name.
- You can be held responsible for any malicious acts by anyone to whom you have given your password.
- Try to include numbers as well as letters in the password
- Take care that no-one can see you type in your password
- Change your password regularly, and certainly when prompted. Also change it if you think that someone may know what it is.

Many database systems, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

- Lock your computer keyboard when you are away from it for any length of time.

Use of E Mail and Internet

- To avoid a computer virus arriving over the Internet, do not open any flashing boxes or visit personal websites.
- Do not send highly confidential or sensitive personal information via e mail
- Save important e mails straight away
- Unimportant e-mails should be deleted straight away.
- Do not send information by e-mail that breaches the Data Protection Act. Do not write anything in an e mail which could be considered inaccurate or offensive, and cannot be substantiated

Electronic Hardware

- All hardware held within The Family School should be included on the asset register.
- When an item is replaced, the register should be updated with the new equipment removed or replaced.
- Do not let anyone remove equipment unless you are sure that they are authorised to do so
- In non-secure areas, consider using clamps or other security devices to secure laptops and other portable equipment to desk tops.

***Disposing of hardware*.**

Computers to be disposed of must be completely 'cleaned' before disposal. It is not enough just to delete all the files*.*

Home working guidance

If you work outside the School or at home, the guidance is the same as given above, However, you may need to consider these extra points. Information is more liable to be lost or stolen outside the school:

- Do not access confidential information when you are in a public place, such as a train and may be overlooked.
- Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people.
- If you use a laptop:
    - Ensure that it is locked and passworded to prevent unauthorised access.
    - Make sure that you don't leave your laptop anywhere it could be stolen. Keep it with you at all times and secure it when you are in school.
    - When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder.
    - *If you are using your own computer, ensure that documents cannot be accessed by others. When you have completed working on them, transfer them back to The Family School and delete them from your computer.*

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the School

Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Glossary of legislation

The Data Protection Act 1998

The Freedom of Information Act 2000

The Environmental Information Regulations 1992

The Human Rights Act 1998

The Regulation of Investigatory Powers Act

Copyright and Intellectual Property rights

The Computer Misuse Act