NORTHFLEET SCHOOL FOR GIRLS
CO-OPERATIVE LEARNING TRUST

PROCEDURE ON

Data Protection
&
Data Security

Date of Policy:	**April 2015**
Member of staff responsible:	**Mr R Chilcott, Network Manager**
Review Date:	**September 2021**
Reviewed:	**September 2019**

The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

Northfleet School for Girls collects and uses large amounts of personal information about staff, pupils, parents and other individuals who come into contact with the school. 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 school complies with its statutory obligations.

Schools have a duty to be registered as Data Controllers with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, which summarises the information held on pupils, why it is held and the other parties to whom it may be passed.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

Information considered personal and sensitive includes:

- All information with pupil and staff names with contact addresses and/or telephone numbers or national insurance numbers
- Annual Review Reports
- References
- Assessment data
- Medical information
- Assessments and correspondence with other agencies (Social Services, EdPsych, Therapies, etc)
- All information relating to Child Protection issues
- All information relating to health, working practices, assessment, performance and salary of staff
- Accident/Incident Books
- Photographs, media or documents containing photographs of pupils and/or staff.
- Fee collection and research data relevant to the school.
- Information required by law to comply with statutory obligations of Local Authorities, Government Agencies or other bodies.

Personal and sensitive information covers information that may be held as paper copies, on CD or DVD, on a memory stick/pen/flash drive, on a portable hard drive, on a network (such as the school server) or on a Learning Platform (such as Fronter).

Personal and sensitive information must not be stored on PC or laptop hard drives or any portable hard drive or memory pen that may be taken or used outside of school unless it is encrypted.

Location of Information & Data

Personal and sensitive information, whether in hard copy or electronically on media, must be stored so that it is out of sight and preferably in a locked area. The exception is medical information where immediate medical attention may be required and it is recommended that such information is available to staff but not visitors or students.

Such information should not be removed from site. However it is accepted that teachers and senior staff may require to transport information between school and their homes in order for school paper work to be dealt with during evening and weekends, or for off-site meetings. The following should then be applied:

- Hard copies of personal information should not normally be taken out of school. Pupil/staff personnel files should never be taken out of school.
- If paper information is taken out of school it should never be left unattended in a way that it could be viewed by others. In addition, personal information should not be left on a PC/laptop screen (the screen should be locked or closed if you move away from the machine).
- Personal information should not be present on laptop hard drives (see Acceptable Use of ICT Policy for full details)
- Unwanted copies of personal and sensitive individual information should be disposed of by shredding in all instances. (This includes hand written notes).
- Extreme care should be exercised when using printers and photocopiers to ensure that information is not left unattended.

Data in the Cloud

The school will select a Cloud Provider who is able to provide evidence of their Data Protection Compliance and within the European Economic Area (EEA) regulation by facilitating the use of the DfE self certification checklist.

The school will make every effort to ensure that any personal data field is not used for the purposes of direct marketing.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection for rights of freedoms of data subjects in relation to the processing of personal data.

Responsibilities

The school must:

- Manage and process personal data properly
- Protect the individual(s) right to privacy
- Provide an individual with access to all personal data held on them.

The school has a legal responsibility to comply with the Data Protection Act. The school, as a corporate body, is the name Data Controller under the Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

The school is required to "notify" the Information Commissioner of the Processing of Personal Data. This information will be included in a public register which is available on the Information Commissioners website site at:
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

Every member of staff that holds personal information has to comply with the Act when managing information.

General Statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared (this is known as a Privacy Notice)
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done appropriately and securely
- Ensure that clear and robust security measures are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded (paper files or computerised)
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Mr R Chilcott, Network Manager, who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk, which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website

Appendix 1

Northfleet School for Girls

Procedures for responding to subject access requests made under the Data Protection Act 1998

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

1. Requests for information must be made in writing, which includes email, and be addressed to the Headteacher**.** If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
   - passport
   - driving licence
   - utility bills with the current address
   - Birth / Marriage certificate
   - P45/P60
   - Credit Card or Mortgage statement
   -

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records, schools can charge up to £10 to provide it.
- if the information requested is only the educational record, viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However the 40 days will not commence until after receipt of fees or clarification of information sought

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school.
Before disclosing third party information consent should normally be obtained.
There is still a need to adhere to the 40 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover.
The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact Mr C Norwood, Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone the school on 01474 831020.