**Margaret McMillan Nursery School and Children's Centre**
Hornsey Rise
Islington
N19 3SF
020 7281 2745
www.margaretmcmillan.islington.sch.uk

# Data security Policy

## Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature
It is the responsibility of all members of the school community to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office, for both the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

It is important to stress that data security applies to all forms of data, regardless of whether it is held on paper or in electronic format.

## Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers, e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data, e.g. class lists, pupil / student progress records, reports, references
- Professional records, e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

## Responsibilities

The school's Senior Information Risk Officer (SIRO) is the head teacher, Mary Hart. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- decide what information is held, for how long and for what purpose,
- track how information has been amended or added to over time, and
- decide who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

### Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

### Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers at admission

### Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through: (schools should amend or add to as necessary)

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from the Senior Leadership Team

### Risk Assessments

Information risk assessments will be carried out the SIRO to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

### Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear that the key contact for key school information is the headteacher
- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
- Staff know to report to the head teacher any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record
- Information about children will be shared with parents but only about their child
- All staff are aware that they should not pass on information about children or their parents/carers indiscriminately. Staff must check that they have parental permission to pass on information about their child before they do so.
- Any external request for information about parents or children needs to be given to the head teacher and she will decide if any information can be shared and by whom.
- Staff should consider the suitability of the surroundings and the presence of other people when they have conversations with children, other staff, parents or carers that may need to be kept confidential. For example avoid making telephone calls in open offices/reception.

- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  - staff,
  - governors,
  - outside users, e.g. ACL. therapists

  This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any MIS data. We use our own system for transfer of reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution so senior staff can access sensitive and other data from home, without need to take data home.

- When personal data is stored on any portable computer system, USB stick or any other removable media the data must be encrypted and password protected. Personal data can only be stored on school equipment (this includes computers and portable storage media where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

- Staff must not allow family or friends to use school owned equipment and must ensure they do not have access to school data.

- School staff with access to setting-up usernames and passwords for email and network access are working within the approved system and follow the security processes required by those systems.

- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

**Technical or manual solutions**

- Staff have secure area(s) on the network to store sensitive documents or photographs, i.e. My Documents folders.

- We require staff to lock their computer when leaving it, even if only for a short time, and log-out of systems when leaving their computer.

- We use encrypted flash drives if any member of staff has to take any sensitive information off site.

- We use encrypted PDFs to transfer data, such as references, reports of children, to schools and partners in Health and Social care.

- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area

- All servers are in lockable locations and are managed by DBS-checked staff.

- We lock any back-up tapes in a secure, fire-proof cabinet. Back-ups are encrypted. No back-up tapes leave the site on mobile devices.

- We use a remote secure back-up for disaster recovery on our admin systems.

- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of system hard drives where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.

- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

- Paper based sensitive information is shredded or incinerated.

- When sending information via email we ensure that any data which could identify the person is encrypted and password [protected.

- Provision has been made for keeping information held in the school confidential. Paper records are kept securely by locking them away and digital information is protected via the school's e-safety policy guidance.

- All email carries a signature disclaimer