# Norden Community Primary School

## Data Protection Policy



September 2015
To be reviewed September 2016

# 1. Introduction

Norden Community Primary School is committed to protecting the privacy of individuals and handles all personal data in a manner that complies with the Data Protection Act 1998 (DPA 1998). The school has established this policy to support this commitment.

In order to operate efficiently, Norden Community Primary School has to collect and use information about people with whom it works. These may include pupils and parents, members of the public, current, past and prospective employees and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of local and central government.

Everyone managing and handling personal information needs to understand their responsibilities in complying with the Data Protection Act 1998 (the Act).

It is the personal responsibility of all employees (temporary or permanent), contractors, agents, students and anyone else processing data, or who has access to personal or sensitive information, to comply with this policy. For the purpose of this document, the above will be referred to as 'employees.'

This policy continues to apply to employees and individuals, even after their relationship with the school ends.

This policy covers all personal data, however they are held, on paper or in electronic format. The policy supports the rights of individuals (data subjects) who wish to see information the school holds about them (by submitting a Subject Access Request). It is a legal requirement that the school complies with the Act, and all members of staff have a statutory responsibility to ensure the schools legal compliance.

This policy is intended to facilitate compliance and all staff should be aware of its content and the key requirements of the Act. Managers should ensure that staff are provided with the appropriate knowledge and training to ensure they can fulfill their responsibilities.

# 2. Responsibilities

Whilst the Head and Governing Body are ultimately responsible, both personal and corporate responsibility applies. All employees are therefore responsible for ensuring compliance with the Principles of the Data Protection Act by complying with this policy.

Managers must ensure that those staff managing and handling personal information are adequately trained and supervised with regard to the requirements of this policy.

# 3. Notification with the Information Commissioners Office

Whist the data that the school hold can be very useful in improving the service which the school provides, it has a duty of care for how it handles and controls access to the sensitive and personal information and data which it holds.

Schools have a responsibility to register as a 'Data Controller' with the Information Commisioners Office (ICO). It is the schools responsibility to ensure that they hold a current registration with the ICO for Data Protection. As a commitment to this registration, they will be complying with the Data Protection Act 1998, with guidance from the local authority. Further information can be found within the following link - http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx

# 4. Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner is the headteacher who is familiar with information risks and the organisation's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities.

- They own the information risk policy and risk assessment.
- They appoint the information asset owners (IAOs).
- They act as an advocate for information risk management.

## 5. Information Asset Owner (IAO)

The School should also identify an IAO for each asset or group of assets within school. For example, the school's management information system should be identified as an asset and should have an IAO. The role of an IAO is to understand:

- What information is held, and for what purposes.
- How information will be amended or added to over time.
- Who has access to the data and why.
- How information is retained and disposed off.

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. There may be several IAOs within an school whose roles may currently be those of e-Safeguarding coordinator, ICT Manager or Information Systems Manager.

Although a school will appoint these key roles, the handling of secured data is everyones responsibility, whether they are an employee, volunteer, technical support or third-party provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even provoke legal action.

All employees must understand their responsibilities and the implications of not acting appropriately when handling sensitive and personal information, which may lead to disciplinary action.

## 6. Definitions of Personal & Sensitive Data

For the purposes of the Act, and the schools Data Protection Policy, it is safest to assume that all information about a living, identifiable individual is personal data and should be dealt with accordingly.

**Personal Data** is information which relates to a living individual who can be identified:

- From this data, or
- From this data when combined with other information which is either in the schools possession or likely to come into the schools possession

**Sensitive Personal Data** can include information relating to:

- Religious belief
- Sexual life
- Physical or mental health conditions
- Member of a trade union
- Political opinions
- Commission or alleged commission of an offence
- Proceedings for any offence committed or alleged to have been committed

Sensitive data must only be collected and used for approved purposes (e.g. Equal Opportunities monitoring) and access to this data must be restricted to those who have a need to know.

## 7. Safeguarding the Rights of Data Subjects

Individuals have various rights under the Act. These are: -

- The right to be told that processing is being carried out
- The right of access to their personal data

- The right to prevent processing in certain cases
- The right to have inaccurate or incorrect information corrected, erased or blocked from processing.

## 8. Processing Personal Data

The definition of processing in relation to data protection is very wide. Obtaining, holding, filing, organising, transmitting, retrieving, disseminating, disclosing and destroying of data are all deemed to be processing in addition to any other process that is carried out on the data.

Employees and others acting on behalf of the school must only have access to personal data that are necessary in order to carry out their duties and responsibilities.

If data are provided by an outside agency then the agency must be asked to confirm in writing that the data were obtained fairly and lawfully, in compliance with the Act.

Where personal data are provided for the purpose of placing a contract to which the data subject is a party then such data is considered to be fairly and lawfully obtained.

## 9. The Principles of the Data Protection Act 1998

The eight principles which form the basis of the Act state that data must be:

**Principle 1 - Fairly and lawfully processed**

Data must be processed fairly and lawfully. Nobody should be deceived or misled about the purpose for which their data is to be processed. Privacy Notices should be included when collecting individual's data. Where appropriate, consent should be obtained from the individual or guardian to process their data.

All forms used to obtain personal data, such as application forms or registration forms must ensure that a Privacy Notice is included and cover the following:

- State the purpose/s for which the information is required.
- Inform the individuals how their information will be used, and where necessary, who their information will be shared with.
- Be reviewed regularly to check that all of the information asked for is still required and necessary.
- Be checked for the accuracy of the data before they are used for any processing. If in doubt about the accuracy of the data they should be referred back to the data subject for confirmation.

Personal data must be collected and handled in a way that complies with the Act and meets the eight principles above. This imposes a duty on the school to ensure that individuals are made aware of the uses that will be made of the information that they supply.

**Principle 2 - Processed for limited purposes**

Personal data can only be obtained for specified and lawful purposes. Data collected for one specific purpose may not then be used for another different purpose.

Data must be used only for the declared purpose/s, which the school has notified to the Information Commissioner's Office. If there is a new purpose or change to an existing purpose then the school must notify the Information Commissioner's Office immediately. Processing of data cannot begin for the new or amended purpose until the Commissioner has accepted this notification.

**Principle 3 - Adequate, relevant and not excessive**

The data must be sufficient to meet their purpose but not provide more information than the purpose requires, or provide information outside the scope of the purpose.

The school must process only that information which is necessary to fulfill the business

requirement or which is needed to comply with legal requirements. For example, it is not necessary to ask about a driving licence on a job application form if the post applied for does not entail any driving duties.

**Principle 4 - Accurate**
The personal data must be accurate when recorded, and accuracy must be maintained throughout the lifecycle of the data.

Errors in personal data that cause data subjects damage or distress could lead to the school being prosecuted. It is important therefore that all appropriate measures are put in place to verify the accuracy of data when they are collected, especially when any significant decisions or processes depend upon the data.

There is a requirement to ensure that data are kept up to date throughout the lifecycle of the data.

**Principle 5 - Not kept for longer than is necessary**
Personal data must not be kept for any longer than is necessary for the purpose for which it was obtained. If data are kept for too long, the accuracy and relevance may be compromised.

Retention periods should be defined for personal data and procedures put in place to ensure compliance. Retention periods must be for clear business purposes and must be documented to identify why certain records are retained for certain periods of time.

When no longer required, data must be deleted or disposed of securely.

**Principle 6 - Processed in line with the rights of the subject of the data**
All individuals (including staff and pupils) have the right to access their personal data that the school may hold about them, this is known as a 'Subject Access Request' (see Section 10). Individuals can request the termination of any processing that causes or is likely to cause them distress. They can insist that their data is not used for marketing and other purposes, and can request that inaccurate data is amended.

**Principle 7 - Stored and processed securely**
All necessary measures must be taken to prevent unauthorised or unlawful processing of personal data and to protect personal data against loss, damage or destruction. (see Section 11)

**Principle 8 - Not transferred to countries without adequate protection**
Personal data must not be transferred to a country outside the European Economic Area (i.e. the EU member states, Norway, Iceland and Liechtenstein) unless that country has in place a level of data protection comparable to that in the EU.

# 10. Subject Access Requests

The school must make available details of how individuals can request access to their data, by means of a Subject Access Request (SAR). SAR's must be made in writing and sufficient detail must be obtained to ensure that the request has been made by the data subject in person.

As proof of identity, at least two identifying documents of the data subject, such as, a birth certificate or passport must accompany the request. If a third party is making the request, a signed letter of consent from the data subject should also be enclosed.

A young person over 16, but under 18, or a child under 16 who is considered to be Fraser Competent (NSPCC Website) may exercise their right of access to his/her information under the DPA.

The person with parental responsibility also has a right of access to the records. However, schools must be particularly careful to verify that the young person has either initiated such a request or consented to such a request being made or that the young person's lack of understanding requires a parent or guardian to act on their behalf.

Another important aspect may well be the nature of the personal information that will be supplied. This will be of particular significance where the information may contain reference to the parent or guardian within the young person's records, for example, where allegations of abuse have been made against the parent or guardian in a social work file. Schools will need to handle requests from minors carefully. Consideration needs to be given to balancing the harm that might arise against the possible benefits of supplying the information

A solicitor can also make a SAR on behalf of their client. The SAR must be valid and the solicitor must also provide written consent/proof of authority to act on the individual's behalf.

It is not permitted to give personal data to third parties unless it is already in the public domain, or authorised by the data subject.

- SAR's must be satisfied within **40 calendar days** of their receipt by the school.

Some SAR's may require further information, or clarification of the information requested, before the process can commence. This information must be requested as soon as possible after the original request has been made. If this additional information is not received within 3 months, the request should be closed and a new request will have to be made.

In certain circumstances, the courts, police or Inland Revenue may have the right of access to personal data without prior permission or knowledge of the individuals concerned.

Subject Access may also include access to images captured by CCTV if an individual is clearly identifiable.

While in principle students have a right of access to the whole of their educational records, in exceptional cases some information may be withheld. The main exemptions are for information which might cause harm to the physical or mental health of the student or a third party, information which may identify third parties (for example other students, although not teachers in this instance), and information which forms part of court reports. Information may also be withheld if it would hinder the prevention and detection of crime or the prosecution or apprehension of offenders if provided.

If a request for information under the DP Act is refused or ignored, the matter can be referred to the Information Commissioner or an application for disclosure can be made to a court.

Schools must keep a record of all subject access requests. This is necessary for a number of reasons including: awareness as to who has made requests, providing an audit trail of events for handling complaints or for onward notification of data errors. In the event that an error is found in personal information, the school may need to take action to contact everyone to whom it has disclosed the data to inform them of the necessary correction.

In addition to the subject access right which can be exercised by students or by parents acting on behalf of students, parents have their own independent right of access to the official educational records of their children under separate education regulations.

**Scale of Subject Access Fees**

There are 2 different sets of charges that can be applied to SAR. The school needs to decide which charging regulations they will use:

- A one off **charge** of £10 for all documents
- Per Page Charges

| No of Pages | Maximum Fee | No of Pages | Maximum Fee |
|---|---|---|---|
| 1-19 | £1 | 100-149 | £10 |
| 20-29 | £2 | 150-199 | £15 |

| | | | |
|---|---|---|---|
| 30-39 | £3 | 200-249 | £20 |
| 40-49 | £4 | 250-299 | £25 |
| 50-59 | £5 | 300-349 | £30 |
| 60-69 | £6 | 350-399 | £35 |
| 70-79 | £7 | 400-449 | £40 |
| 80-89 | £8 | 500+ | £50 |
| 90-99 | £9 | | |

For further information about The Education (Pupil Information) (England) Regulations, please see the following link - http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/technical_guidance_note_access_to_pupils_information_held_by_schools_in_england.pdf

# 11. Keeping Data Secure

The school acts as custodian of personal data and must therefore ensure that necessary and sufficient precautions are in place to prevent misuse or unauthorised access to data as well as having security measures in place to prevent loss or damage to data.

An information breach would be caused when (and this not an exhaustive list):

- A fax containing sensitive information is sent to the wrong number
- A laptop containing personal data is lost or stolen
- A USB (memory stick) containing personal data is lost or stolen
- A vehicle containing a laptop or paper files is stolen
- A laptop or paper files are stolen from a private property
- An email is sent (either internally or externally) with files attached containing personal data and the email is sent to the wrong email address
- An email is sent (either internally or externally) with files attached that contain personal data which is far in excess of that necessary in order for the business function to be carried out
- Personal data is shared outside of the work place for a legitimate business reason, but it is lost by the recipient or it is stolen from the recipient, or it is used by the recipient in a manner for which they have no authority for
- Personal data is transferred electronically outside the workplace and is not encrypted when it should be
- Paper files of personal data are left unattended and are taken or copied and then used for an unauthorised purpose
- A member of staff uses personal data for a personal rather than a work related business reason.

| **Key Requirements** | |
|---|---|
| All removable media devices, such as, USB/Memory Sticks, Laptops etc, **must** be encrypted. | |
| All staff must adopt a 'clear desk' policy to ensure that no paper work or electronic devices are left unattended. | Filing cabinets containing personal data must be locked outside of normal working hours and keys must be held securely by nominated staff. |
| All such electronic data must be stored in secure server areas, not on computer hard drives, laptops or other mobile devices. | Any electronic data backed up to media such as CD must be kept physically secure. |
| If any data are to be taken from the office (e.g. to work at home) then the data must be held securely at all times whilst in transit and at the location they are being held. In particular data must be protected from unauthorised access. | |

Electronic files must be password protected and passwords must be changed on a regular basis.

Passwords must contains a minimum of 7 characters and must contain at least 3 of the following characteristics:

- Latin uppercase letters (A through Z)
- Latin lowercase letters (a through z)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters such as: exclamation point (!), dollar sign ($), number sign (#), or percent (%).

Where outside bodies process or hold any of the schools personal data then the school must be satisfied that the data is held securely and with due regard to the obligations of the Act.

## 12. Disciplinary Action & Criminal Offences

Although SchoolName is responsible for complying with the DPA, **employees may face internal disciplinary action** if they cause the school to be in breach of its obligations by failing to follow policies and guidance.

The DPA also creates a range of criminal offences for which employees may be found personally liable, including:

- Unlawfully obtaining, disclosing or procuring the disclosure of personal data
- Selling, or offering to sell, personal data which has been unlawfully obtained.

## 13. Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.