Data Protection Policy & Freedom of Information

Data Protection Policy

Rendell Primary School collects and uses 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, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Enforcement by the ICO

- Complaint to ICO
- ICO audit (currently only with consent)
- Powers of Assessment
- ICO may serve
    - Undertaking
    - An information notice
    - An enforcement notice
    - Monetary penalty notice: max £500.00 fine (for serious breaches of a principle likely to cause substantial damage or distress
- Certain Criminal offences

MPN's Common mischiefs

- Loss or theft of unencrypted devices (laptops, USB sticks etc)
    - Highest fine to date £150,000
- Loss or theft of paper records
    - Highest fine to date £150,000
- Failing to dispose of records securely
    - Highest fine to date £200,000
- Faxing to the wrong recipient
    - Highest fine to date £100,000
- Email errors (ie reply to all) etc
    - Highest fine to date £120,000
- Postal errors (ie mailing data to the wrong person)
    - Highest fine to date £140,000
- Insecure websites/networks
    - Highest fine to date £250,000

Examples of the above

2012 – Durham University. Undertaking- screen shots containing personal data published in online training

2011 – Phoenix Nursery – loss of an unencrypted backup tape and accompanying device containing details of pupils, parents & guardians

2011 Bay House School – school systems hacked due to staff *using identical passwords* to access database and website. Personal data and medical data exposed
2011 Freehold Community School Oldham – theft of unencrypted laptop from a teacher's car.

ICO and schools
2012 ICO study of the level of data protection compliance in schools

- ICO publishes its findings in a report 'Significance for the education sector'
- 'Your rights to your information' – new ICO initiative launched. Teaching materials and lesson plans available to give teachers an introduction to Information Rights. Aim: to embed information rights and privacy into the curriculum. www.ico.org.uk/youth

What does the Data Protection Agency do?

- Regulates the processing of personal data relating to living individuals (**data subjects)**
- Imposes legal obligations upon **data controllers (**person or organisation that controls the processing of personal data**)**
- Provides data subjects with legal rights in respect of the way their **personal data** is processed.
- Introduces criminal and civil sanctions for breaches
- Enforced by the Information Commissioner's Office (ICO)

Data Protection Terminology

- **Personal data:** electronic or manual information which identifies a living individual. It includes opinions about the data subject and intentions towards them.
    - Eg. Name, address, email address, DNA sample, CCTV image, pupil file, pupil photo on website, emails between staff about a pupil or parent, pupil photos on staff smart phone.
- **Sensitive personal data: personal data relating to the data subject's :**health (physical or mental); racial or ethnic origin, religious or philosophical beliefs; trade union membership; sexual life; commission of criminal offences
    - Eg a pupil's health records**:** epipen prescription.

School's 3 Main Obligations

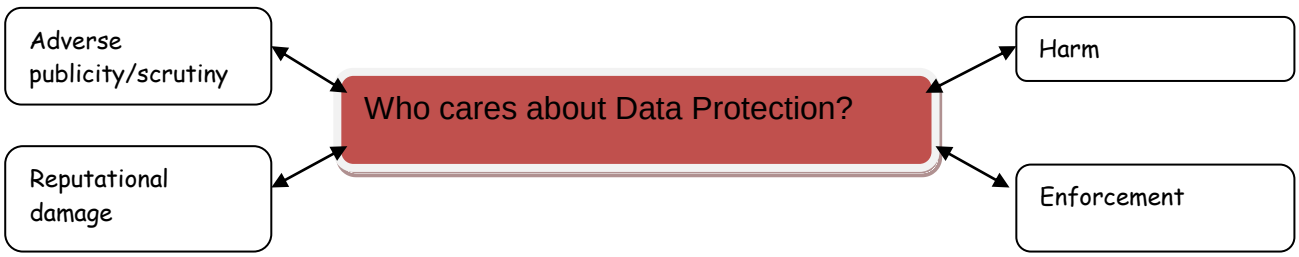
1. Registration/Notification
2. Comply with the 8 data protection Principles
    a. Set the standard by which the school must process personal data
    b. Processing line with the Principles is the key to compliance
3. Process personal data in line with data subjects legal rights.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act following the 8 Data protection principles detailed below 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.

The Information Law Practice 2013



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.

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;
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. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
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.

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
- 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 so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- 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

Examples of '**Hot Spots'**

- Pupil biometrics – Engages the DPA and also a new law the Protection of Freedoms Act 2012 (POFA)
    - Complies with all 8 principles POFA and you will need to notify and obtain parental permission/consents before biometric processing begins. If one parent objects and the other consents you cannot process
    - Child objection
- Cloud computing – applications hosted and delivered over the internet.
    - Is your CSP a data processor? You must obtain evidence.
    - Beware false claims
- Photographs – does the DPA apply?
    - Is the photo for school, media or personal use?
    - Official school use: photos taken for official school use are likely to be covered. Ie library cards, passes, pupil files.
    - Group photos: grey area – DPA may or may not apply depending upon whether pupil image amounts to personal data. Safer to assume that DPA applies.
    - Media photos- make sure that pupils and parents are aware that photos taken may appear in the newspaper in advance of the photo being taken by the journalist.
    - Personal use – photos and videos taken for the family album and purely personal use are likely to be exempt from the DPA (section 36 'domestic purposes' exemption.) Family album.
- How would you define the family album?

    - Photos taken by pupils and parents. Can you control where they end up? Social networking …. Facebook, you tube twitter.
    - Section 36 DPA – Educate children and parents.
- Rendell's policy of taking photos or videos of children in school is:
    - Photographs can be taken provided they are for family and personal friends only.
    - Photographs or short video clips taken on smartphones in school that have any other children in them must not be published on any media site such as websites, Facebook or You Tube; or in any newspaper.
    - If a parent or carer wishes to take video footage other than on a mobile phone, they must complete a request form available from the school office and sign to say that it is for personal use only and will not be used for publishing in any way.
- Police requests for data – power v duty?
    - Always should be in the form of written requests.
    - Would your failure to disclose prejudice prevention or detection of crime?
    - Fishing expeditions
    - Court order
    - Other prosecuting agency.
- CCTV – DPA likely to apply
- Therefore the 8 principals apply
- CCTV privacy notice
    - What will you use the footage for?
    - Accuracy and retention of footage
    - Subject access requests
    - CCTV code of practice (revised edition) www.ico.gov.uk
- BYOD – (Bring your own device) Employees who bring their own devices into the workplace for use and connectivity to their employers network : smartphones, laptops, ipads, USB sticks.
    - The school remains in control of the personal data for which it is responsible regardless of the ownership of the device used to carry out the processing.
    - BYOD increase the security risk.
- ***Rendell Primary Schools policy on BYOD is:***
    - Only memory sticks that are encrypted and provided by the school can be used for transporting data and information
    - Any personal devices used in school must not contain personal images or data on any pupils
    - Use of personal devices to access emails is permissible provided security settings ensure that the emails are not accessible by any third party.
    - No information is to be stored in Cloud services other than those authorised by the school.
    - The school takes no responsibility for loss or damage to any personal devices.
    - Lost or stolen devices should be reported to the management of the school if there is any probability that data security related to school might be breached.
    - If a member of staff leaves employment then any links to school emails etc should be immediately removed from personal devices.

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 3 years. The policy review will be undertaken by the Headteacher, or nominated representative.

Rendell Primary School – Freedom of Information requests

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

Rights of access to information (Freedom of Information) FOI

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 Mrs K Rixon**.** 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, dependant 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 £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. Parental Right of Access to Educational record - as an Academy we are technically subject to the regulations. However many academies still observe the spirit of the regulations.

5. The response time for subject access requests, once officially received, is 40 calendar 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 and further information about identity or location of information has been received.

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 Mrs K Rixon, Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk.