Pensby Primary School

Data Protection and Data Security Policy

General Data Protection Regulation (GDPR)

September 2018

Data Protection Policy and Procedures

Schools handle increasing amounts of personal information and have a statutory requirement to comply with The Data Protection Act 1998("DPA"). Schools should have clear policies and procedures for dealing with personal information, and be registered with the Information Commissioner's Office ("ICO"). Schools should have systems in place to reduce the chances of a loss of personal information, otherwise known as a data breach which could occur as a result of theft, loss, accidental disclosure, equipment failure or hacking.

Contents

Introduction

1. Aims & Objectives:

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- The law regarding personal data;
- How personal data should be processed, stored, archived and deleted/destroyed;
- How staff, parents and pupils can access personal data.

Pensby Primary School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR). The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services. This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR. Organisational methods for keeping data secure are imperative, and Pensby Primary School believes that it is good practice to keep clear practical policies, backed up by written procedures.

1.1. It is a statutory requirement for all schools to have a Data Protection Policy: (http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools)

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR);
- The Freedom of Information Act 2000;
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016);
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004;
- The School Standards and Framework Act 1998.

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)' ;
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'.

This policy will be implemented in conjunction with the following other school policies:

- The Schools Retention Policy
- Whistleblowing Policy
- Business continuity and Disaster Recovery plan

1.2. Data Protection Principles

The Data Protection Act 1998 establishes eight 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.

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

1.3 Data protection officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws;
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members;
- The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools;
- The DPO will report to the highest level of management at the school, which is the Headteacher;
- The DPO will operate independently and will not be dismissed or penalised for performing their task;
- Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations

2. Data Types

Not all data needs to be protected to the same standards, the more sensitive or potentially damaging the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are

assessed, controlled and managed. A similar process should take place with managing school data. The DPA defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a " Potential Data Breach" which could result in legal action against the school. The loss of sensitive personal data is considered much more seriously and the sanctions may well be more punitive.

2.1. Personal data

The school 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 eg names, addresses, contact details, legal guardianship contact details, disciplinary records;
- Curricular / academic data eg class lists, pupil / student progress records, reports, references;
- Professional records eg employment history, taxation and national insurance records, appraisal records, disciplinary records and references;
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

2.2. Sensitive Personal data

Sensitive personal data is defined by the Act as information that relates to the following 8 categories: race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexual life and criminal offences, criminal proceedings. It requires a greater degree of protection and in a school would include:-

- Staff Trade Union details
- Information on the racial or ethnic origin of a child or member of staff
- Information about the sexuality of a child, his or her family or a member of staff
- Medical information about a child or member of staff
- Information relating to any criminal offence of a child, family member or member of staff.

Note – On some occasions it is important that medical information should be shared more widely to protect a child - for instance if a child had a nut allergy how it should be treated. Where appropriate written permission should be sought from the parents / carers before posting information more widely, for instance in the staff room.

2.3. Other types of Data not covered by the act.

This is data that does not identify a living individual and therefore is not covered by the remit of the DPA this may fall under other access to information procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school which does not relate to an individual. Some of this data would be available publically (for instance the diary for the forthcoming year), and some of

this may need to be protected by the school (If the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

The ICO provide additional information on their website See
http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

3. Responsibilities

The Headteacher and Governing Body are responsible for Data Protection.

3.1. Risk Management - Roles

The school's DPO is - Sarah Webb, Head of Business Development, E2E Integration Limited

They:

- determine and take responsibility for the school's information risk policy and risk assessment;
- appoint the Information Asset Owners **(IAOs**).

The school will identify Information Asset Owners (IAOs) . In this school they are:
The Headteacher and Data Protection Governor. The IAOs act as Data Controllers. The schools Data Processor is Mrs K Yeardsley-Jones.

The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose;
- how information as been amended or added to over time, and
- who has access to protected data and why.

3.2. Risk management - Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner.
- Everyone in the school is expected to follow all processes and procedures in handling data;
- 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.

4. Legal Requirements and lawful processing

4.1. Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.
http://ico.org.uk/for_organisations/data_protection/registration

The legal basis for processing data will be identified and documented prior to data being processed.

4.2 Lawful processing

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:

- Compliance with a legal obligation;
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- For the performance of a contract with the data subject or to take steps to enter into a contract;
- Protecting the vital interests of a data subject or another person;
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks).

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law;
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent;
- Processing relates to personal data manifestly made public by the data subject;
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement;
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards;
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of 6 health or social care systems and services on the basis of Union or Member State law or a contract with a health professional;
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices;
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

4.3. Information for Data Subjects (Parents, Staff)

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students and staff 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 through a letter – which may be sent in paper form or put on the school website. See Appendix 2

4.4 consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes;
- Where consent is given, a record will be kept documenting how and when consent was given;
- The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease;
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time;
- The consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

4.5 The right of access (SAR – Subject Access Requests)

- Individuals have the right to obtain confirmation that their data is being processed;
- Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing;
- The school will verify the identity of the person making the request before any information is supplied;
- A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format;
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information;
- All requests will be responded to without delay and at the latest, within one month of receipt;
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request;
- Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal;
- In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

4.6 The right to rectification

- Individuals are entitled to have any inaccurate or incomplete personal data rectified;
- Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible;
- Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to;
- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex;

- Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.
- The request for rectification must be made using the form at the end of this policy.

4.7 The right to erasure

- Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing;
- Individuals have the right to erasure in the following circumstances:

— Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
— When the individual withdraws their consent;
— When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
— The personal data was unlawfully processed;
— The personal data is required to be erased in order to comply with a legal obligation;
— The personal data is processed in relation to the offer of information society services to a child;

- The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

— To exercise the right of freedom of expression and information;
— To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
— For public health purposes in the public interest;
— For archiving purposes in the public interest, scientific research, historical research or statistical purposes;
— The exercise or defence of legal claims.

- As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so;
- Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.
- The request for erasure of data must be made using the form at the end of this policy.

4.8 The right to restrict processing

- Individuals have the right to block or suppress the school's processing of personal data;
- In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future;

The school will restrict the processing of personal data in the following circumstances:

— Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data;
— Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual;

— Where processing is unlawful and the individual opposes erasure and requests restriction instead;
— Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim;
— If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.;
— The school will inform individuals when a restriction on processing has been lifted.
— The request to restrict processing of data must be made using the form at the end of this policy.

4.9 The right to data portability

- Individuals have the right to obtain and reuse their personal data for their own purposes across different service;.
- Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability;
- The right to data portability only applies in the following cases:

— To personal data that an individual has provided to a controller;
— Where the processing is based on the individual's consent or for the performance of a contract;
— When processing is carried out by automated means.

- Personal data will be provided in a structured, commonly used and machine-readable form;
- The school will provide the information free of charge;
- Where feasible, data will be transmitted directly to another organisation at the request of the individual;
- The school is not required to adopt or maintain processing systems which are technically compatible with other organisations;
- In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual;
- The school will respond to any requests for portability within one month;
- Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request;
- Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.
- The request for portability of data must be made using the form at the end of this policy.

4.10 The right to object

- The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information;
- Individuals have the right to object to the following:

— Processing based on legitimate interests or the performance of a task in the public interest;
— Direct marketing;
— Processing for purposes of scientific or historical research and statistics.

- Where personal data is processed for the performance of a legal task or legitimate interests:
- An individual's grounds for objecting must relate to his or her particular situation.

— The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

- Where personal data is processed for direct marketing purposes:

— The school will stop processing personal data for direct marketing purposes as soon as an objection is received;

— The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

- Where personal data is processed for research purposes:

— The individual must have grounds relating to their particular situation in order to exercise their right to object;

— Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

- Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

5. Transporting, Storing and Deleting personal Data

- The policy and processes of the school will comply with the guidance issued by the ICO here

5.1 Information security - Storage and Access to Data

Technical Requirements

- 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.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.
- The school has a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

Portable Devices

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;

- the device must be password protected. Memory sticks and cards are NOT used in this school.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.
- The timetable for changing passwords on all systems is every 6 months.

Images

- Images of pupils will only be processed and transported by use of encrypted devices and permission for this will be obtained in the privacy agreement.
- Images will be protected and stored in a secure area.

Cloud Based Storage

- The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.
  http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

Third Party data transfers

- As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.
  http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

Retention of Data

- The guidance given by the Information and Records Management Society – Schools records management toolkit will be used to determine how long data is retained.
- Personal data that is no longer required will be destroyed and this process will be recorded.

5.2 Systems to protect data

Paper Based Systems

- All paper based OFFICIAL or OFFICIAL – SENSITIVE (or higher) material must be held in lockable storage, whether on or off site.
- Paper based personal information sent to parents will be checked by a member of the senior management team before the envelope is sealed.

School Websites

- Uploads to the school website will be checked prior to publication ensure that personal data will not be accidently disclosed and that images uploaded only show pupils where prior permission has been obtained.

E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

- E-mails containing sensitive information should be encrypted, for example by attaching the sensitive information as a password protected word document. The recipient will then need to contact the school for access to a one-off password
- In accepting a school email address, staff/Governors must ensure it is not for personal use
- In accepting a school email address, staff/Governors may receive unsolicited mail. If you receive unsolicited email on your school account from a company e.g. spam, this should be blocked and a report sent through to the email administrator (right click on the email – select 'add to junk folder' then click report. An unsolicited email from a parent or one from another Wirral employee containing data, must be reported through the 'Data Breach' form in the Data Protection and Security policy.
- If staff/governors send an email to an incorrect person who does not have a Pensby email account,(or 'reply all' or 'forward' the email from a Pensby email knowing non-school email participants are listed) that contains ANY personal data about ANY members of the school community, this must be reported through the 'Data Breach' form in the Data Protection and Security policy
- Groups on the email system will be set up by the technician under the instruction of the Headteacher. These groups begin with pen. E.g pen.admin@pensby-primary.wirral.sch.uk
- Staff are NOT permitted to set up their own groups unless they have the permission of the Headteacher. **Any groups set up by staff prior to this email MUST be deleted immediately.**
- There is a strict protocol in place for allocating emails to staff and removing email accounts when staff leave employment.

Clear Desk and Room Security policy

- All desks are to be cleared of any data. At the end of the day, all data will be locked away in storage cupboards/walls or desks.
- Keys to access locked rooms/cupboards are stored in a security key box in each room at all times.
- Key administration rooms have additional combination locks to present a second line of security.
- Spot checks are undertaken by senior management to ensure the clear desk policy is effective.

6.0 Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach the DPO will be informed by the head teacher and/or chair of governors or vice versa.
- The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- The headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.
- The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case by-case basis.
- In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.
- A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
- In the event that a breach is sufficiently serious, the public will be notified without undue delay.
- Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.
- Within a breach notification, the following information will be outlined:
- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
— The name and contact details of the DPO
— An explanation of the likely consequences of the personal data breach
— A description of the proposed measures to be taken to deal with the personal data breach
— Where appropriate, a description of the measures taken to mitigate any possible adverse effects
- Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

7.0 How Data is collected/stored and updated in Pensby Primary school

- Pensby Primary School Data map details what data we collect and how it is stored. The schools Asset Information register details retention and storage of data.
- Personal data is collected through data collection sheets generated by SIMs. This is an annual process for all pupils and staff.
- If an update to data is required, the current SIMS data sheet is printed, the subject annotates the change in data and signs to indicate their consent
- If a SIMS data sheet will not be suitable for annotating a change in data, the subject is asked to complete the 'Request to Change Data' form in Annex A.

8.0 A summary of Data Security measures and procedures in Pensby school (see Clear Desk Policy section 5.2)

- Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access;
- Confidential paper records are not be left unattended or in clear view anywhere with general access;
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site;
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet or storage wall, drawer or safe when not in use;
- Memory sticks (USBs) will not be used in this school.

- All electronic devices are password-protected to protect the information on the device in case of theft;
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft;
- Staff and governors do not use their personal laptops or computers for school purposes unless they are personally password-protected and fully encrypted;
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password;
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient;
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients;
- When sending confidential information by fax, staff will always check that the recipient is correct before sending;
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data;
- Before sharing data, all staff members ensure:

— They are allowed to share it;
— That adequate security is in place to protect it;
— Who will receive the data has been outlined in a privacy notice.

- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times;
- The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place;
- Pensby Primary School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action;
- The school business manager/Office manager (SBM) is responsible for continuity and recovery measures are in place to ensure the security of protected data;
- Pupils assessment information is held on SPTO. This is password protected and encrypted and only accessible to relevant staff. Governors have access to SPTO but data is anonymised;
- Pupil data is held within SIMS. SIMS access is password protected and passwords are only distributed to relevant staff;
- TUCASI holds data about pupils and families. access is password protected and passwords are only distributed to relevant staff;
- The school utilises a strong system of firewalls to deter any internet attack;
- All staff emails are password protected;
- All devices that can access pupil, staff details are password protected. They lock after 5 minutes of inactivity;
- Staff access cards are monitored and any loss reported results in deletion from entry system.

9. Policy Review Reviewing:

This policy will be reviewed, and updated if necessary every two years.

Date: Review: Signed:
Chair of Governors

Annex A
Request to Change data form

Appendix 1 Links to resources and guidance

ICO Guidance for schools
http://ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Research_and_reports/report_dp_guidance_for_schools.ashx
A downloadable guide for schools

Specific information for schools is available here
http://ico.org.uk/for_organisations/sector_guides/education

Specific information about use of Cloud Based technology
http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing

Specific Information about CCTV
http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

Information and Records Management Society – Schools records management toolkit
http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school
A downloadable schedule for all records management in schools

Disclosure and Barring Service (DBS)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/143669/handling-dbs-cert.pdf Details of storage and access to DBS certificate information.

DFE Privacy Notices
https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

DFE Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Appendix 2 Privacy Notice – Pensby Primary School

Pensby Primary School collects an uses pupil information under the Data Protection Act 1998and the Education Act 1996 which are a lawful basis for collecting and using pupil information for general purposes (and from article 6 and article 9 where data processing is special category data from the General Data Protection Regulation from 25th May 2018)

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information
- Special Educational needs information
- Exclusions and behavioural information

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use pupil information under Article 6 of the General Data Protection Regulation:

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

And from Article 9 of the General Data Protection Regulation:

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

Collecting pupil information
Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data
We hold pupil data for the time the pupil is with us in school. Once they have left the data is accessible for various timeframes. Refer to Retention Policy.

Who we share pupil information with
We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- The school nurse/NHS
- Any bodies where we must statutorily share the information e.g. Social Services
- The Soft Federation Schools in The South Deeside Primary Schools Federation

Why we share pupil information
We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact The Head Teacher in the first instance.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact:
Mrs K Brown at Pensby Primary School (Data Proection Administrator) or The Schools Data Protection Officer (DPO) Sarah Webb at e2e Integration customerservice@e2eintegration.co.uk

Appendix 4 Privacy Notice for school workforce

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- Emergency contact details

Why we collect and use this information
We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- Ensure that in an emergency we contact the right person to assist

The lawful basis on which we process this information
We collect and use pupil information under Article 6 of the General Data Protection Regulation:

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

And from Article 9 of the General Data Protection Regulation:

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

Collecting this information
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information
We hold school workforce data for the period of time that staff are employed by us. Information on systems such as SIMS is kept for longer (see retention policy).

Who we share this information with
We routinely share this information with:

- our local authority
- the Department for Education (DfE)
- The Soft Federation Schools in The South Deeside Primary Schools Federation

Why we share school workforce information
We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

South Deeside Primary Schools Federation
We share personal data with schools in the Federation to allow staff the opportunity to work together and share their knowledge and expertise.

Data collection requirements
The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information
If you would like to discuss anything in this privacy notice, please contact:

If you would like to discuss anything in this privacy notice, please contact:
Mrs K Brown at Pensby Primary School (Data Proection Administrator) or The Schools Data Protection Officer (DPO) Sarah Webb at e2e Integration customerservice@e2eintegration.co.uk

Appendix 4 School Procedures

SIMS

- All pupil data is held on the LA SIMS system any additional information (reports etc) is kept in individual pupil files in a locked cupboard. When pupils transfer to other schools all data is sent via secure site set up by the LA.
- All staff information is held on the LA SIMS system. Hard copies of contracts etc sent from the LA is stored in individual staff files and held in a locked cabinet. Information on staff who have left is kept in a locked cupboard.
- Data held within the SIMS system is for current and past pupils/families. Once a pupil transfers out of the school, their data is retained in the SIMS system indefinitely.

FMS

- All financial data is held on the LA FMS system. Purchase Orders and Invoices are kept in a locked cupboard. Data is kept for the appropriate amount of time according to the retention timetable.
- All file storage cabinets are kept closed during the day then locked at the end of the day. Desks are cleared at the end of the day of all filing trays and any documentation is stored away securely including the school diary.
- Storage of old files relating to FMS are kept for the instructed period of time following the Retention of Records Timetable in a locked cupboard.

Pupil and Staff Registers

- Registers are kept in a locked cupboard in the admin office, until they are required.

- Pupil or staff data that is sensitive, that needs to be shared with classroom staff e.g medical information, is situated on the inside of the lockable storage walls so that staff can access it.

Disposal of paper documents

- Shred-it is purchased by the school – they visit every 2 months. There are 2 shred-it bins in the school - one in the main admin office and one in the photocopier room.
- When the shredding boxes are full, spare shredding bags are issued. These are stored in the admin cupboard (and sealed), which is secured at the end of the day. In the rare event of the admin cupboard being full, bags are stored in the meeting room, which is also secured.
- Shred it carry out their work on site and provide written confirmation of the destruction of bags. Shred it provide a GDPR Regulations statement.

Admin IT

- All Admin computers/laptops have a screen saver that activates after 3 minutes.
- Admin staff are instructed that if they are alone in the admin area and need to leave the office unattended then should log out and not wait for the screen saver to activate.

Admin Key storage

- Master keys are stored in a locked cupboard.
- The main keys which unlock the admin cupboard are kept in a keysafe.
- Key staff have master keys of their own – these staff are the Premises Manger, Headteacher, Caretakers. These staff are responsible for ensuring the master keys are kept securely.
- Key staff who may require keys are given the access code to the key boxes. These staff are:

The Headteacher, Deputy Headteacher, all admin staff, premises manager and caretakers.

ICO registration

- We renew our Data Protection Registration with ICO annually.

Visitors

- All contractors and visitors sign-in via an electronic system we have a No Phone Policy.
- All visitors are required to sign in at the main entrance. The glass screen secures the main entrance and is opened on acceptance of visitors.

Classrooms processes

- Classroom laptops and tablets are stored in lockable laptop trollies
- Teachers laptops have access to SIMS. To protect data all staff laptops and the main classroom screens, have a screen saver that activates after 5 minutes. Pupil laptops cannot access SIMS.
- Classroom staff are instructed, that if they leave their classroom empty, they should activate their screen saver rather than wait for the screen saver activation after 5 minutes.
- Any pupil data in paper form is stored away in a lockable storage wall, keys are kept in a key safe. All data is locked away at the end of each day.
- The key safe codes are recorded and kept securely in the admin office. Classroom staff are given the key code so they can access the keys.
- Pupil or staff data that is sensitive, that needs to be shared with classroom staff e.g medical information , is situated on the inside of the lockable storage walls so that staff can access it.

- Lists of pupils names will be seen in the classroom areas, to protect pupils identify this is first names only. In the case of more than one child having the same name, the first letter of the surname will be used.
- Class teachers are responsible for ensuring that their interactive boards are fully switched off at the end of the day.
- Class teachers are responsible for ensuring all paper documents that contain any data, are locked in their storage walls at the end of the day, and the storage wall keys are locked in the classroom key safe.

Kitchen

- Data is held on laptop which is stored away in a locked room at the end of the day. The kitchen is locked prior to the start of kitchen staff arriving and after catering staff leave for the day.
- Pupil or staff data that is sensitive, that needs to be shared with classroom staff e.g medical information, is situated in the kitchen office so that staff can access it. This room is locked.

Children's Club

- Pupil or staff data that is sensitive, that needs to be shared with classroom staff e.g medical information, is situated on the inside of the lockable cupboard so that staff can access it.
- The IT equipment and process for data protection are in line with that in the classroom areas.

Photocopier

- Staff are able to print to the photocopier via their computers. Every class and department has their own unique confidential code. Copies can only be accessed via this code being input directly into the photocopier only.
- Locked printing that has any unprinted documents, deletes after 24 hours.

Photographs

- Photographs taken of pupils in school are stored via SPTO and deleted when children leave the school.
- Staff have a classroom camera. This camera should not leave the site, unless taken on a school visit. Staff should record this on their visit risk assessment.
- Once photographs have been taken, the classroom cameras are locked away at the end of the day. The images are then either uploaded to the school website, or SPTO. Once uploaded all images are deleted.
- The nature of images uploaded to SPTO and the school website is detailed in the schools 'Use of Images' policy that parents/carers read and approve or disapprove.
- Staff are aware that once a photograph is taken on the classroom camera and moved to the SPTO site it is to be deleted.

Governors

- Governors are only communicated with through their school email address.
- Once a governor leaves their email is deleted.
- Only general data is sent via email e.g. whole cohort/class data so that no pupils are identified
- Governors may be given paper documents at meetings that hold personal data. In this case, the document is retrieved at the end of the meeting. These documents are marked 'Strictly Confidential'.

- If a governor leaves their role any data which they hold should be brought into school for shredding. That governor is then asked to sign to confirm that they have no data in their possession.

SPTO / TUCASI / My Concern/3rd party contractors

- The schools uses SPTO, TUCASI and My Concern and these packages contain personal data.
- The IT packages are all password protected.
- Admin staff and the Headteacher have access to TUCASI through passwords.
- All classroom based staff have logins to SPTO. Governors on the SED committee also have logins to SPTO. Their access is limited and all data for those governors is anonymous and no pupil can be identified.
- All staff have a login for My Concern. The Safeguarding governors also have access to MY Concern. Their access is limited and all data for those governors is anonymous and no pupil can be identified
- The Headteacher and office manager are responsible for controlling the distribution of login in details and permissions. The Headteacher controls those for SPTO and My Concern. The office manager controls those for TUCASI.
- Pupils reports are communicated to their families through SPTO. All families are issued with a login and this is controlled by the Headteacher. Parents/carers have full access to their child's academic data, attendance data in SPTO. No paper reports are issues to parents/carers.
- Any other 3rd part contractors that are utilised by the school, that require access to data must share their Data Protection systems, policies and how they comply with GDPR before they are used.

Use of USB drives/external hard drives/removing data from site

- The school does not use USB drives or external hard drives for any purpose. Staff are not permitted to upload any data or school information to USB drives under any circumstances.
- Staff are expected to transport their laptops and pupils books between home and school. Staff are responsible for ensuring that these are kept secure at all times. Laptops and books should be out of view and not easily accessible to anyone.
- At home, when logging into staff emails, SPTO or TUCASI, staff are responsible for ensuring that no person can view any of the material they are looking at.
- My Concern should not be accessed from home, unless in the case on an emergency and the Headteacher has instructed that member of staff to login to report a concern.

Personal cloud based accounts e.g One Drive/ Dropbox etc

- Staff are not permitted to download any school items including documents of images, to cloud based storage such as One Drive or Dropboax.
- Staff are responsible for ensuring that any personal cloud based accounts such as One Drive or Dropbox are not linked to their school devises in terms of accepting downloads.

Emails

- All school staff have school emails that are password protected. These emails are controlled by the IT technician who is instructed to set them up by either the Headteacher or the office manager.
- Once a member of staff leaves their email is deleted.

CCTV

- The school has a CCTV system. Details of how this system is manged can be found in the CCTV policy.
- Images are stored for 30 days, then deleted.
- The schools CCTV policy covers the CCTV system for Pensby and Stanley. This details CCTV permissions for both schools and storage of data.

Data Breaches

If any member of staff or governor, believes that any data they hold has been viewed/taken in any way by someone not permitted to do so, they must report this immediately to the Headteacher. A Data Breach report must be completed immediately. The ICO will be informed.

Appendix 5 Glossary

Data Protection Act 1998: All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO The Information Commissioner's office. This is a government body that regulates the Data Protection Act.
The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England: General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media: General information note from the Information Commissioner on publication of examination results.

Education Act 1996: Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005: Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972: Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998: Retention of school admission and exclusion appeal papers and other pupil records.

PENSBY PRIMARY SCHOOL - DATA BREECH REPORT	
Name and position of person initially making the report	
Date and time of report	
Details of data breech – who? What? Why? Where? When?	
Date and time breech is reported to DPO/ICO OR Date and time Breech is reported to the school by DPO/ICO	
Details of any briefing given to staff, governors - who? What? Why? Where? When?	
Advice received from DPO/ICO	
Any further information following the above stages	
Conclusion and required actions following data breech - who? What? Why? Where? When?	
Evidence that any actions have been completed - who? What? Why? Where? When?	

Pensby Primary School - Security Check List - 2017/18

	Every 6 Months – sign to verify	Every 12 Months – sign to verify
Staff laptop passwords changed		
Admin PCs passwords changed		
Intruder alarm code changed		
Keylock boxes code changed		
Key pad codes on office doors changed		
SIMS passwords changed		
SPTO passwords changed		

Pensby Primary School – Request For Changes in Data

Name of person making request	
Names/ and classes of children in school	
Date of request	
Details of request – (please circle) **Rectification,** **erasure,** **portability,** **restriction**	
Initial request received by and date	
Date request received by Headteacher	
Date request discussed with DPO (if appropriate	
Outcome of request and name of approver	
Details of when/who actioned this request	
Details of when who/informed the person making request of the outcome and actions taken	