**St Mary’s C of E School**

**School Personal Data Handling Policy**



**Date reviewed: July 2015**

**Signed: Headteacher:**

**Signed Chair of governors:**

**Date for next review: July 2016**

**Background to the policy**

Recent publicity about data breaches suffered by organisations and individuals has made the area of personal data protection compliance a current and high profile issue for schools and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to avoid or at least minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

* No school or individual would want to be the cause of any data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
* Schools are “data rich” and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
* The school will want to avoid the criticism and negative publicity that could be generated by any personal data breach.
* The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

It is a statutory requirement for all schools to have a Data Protection Policy. St Mary’s Data Protection policy was passed by governors in March 2012

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. Legislation covering the safe handling of this data is mainly the Data Protection Act 1998 (‘the DPA’). Moreover, following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008, Data Handling Procedures in Government. The latter stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in schools, it is critical that they adopt these procedures too.

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature. (Becta – Good Practice in information handling in schools, 2009 – keeping data secure, safe and legal): <http://webarchive.nationalarchives.gov.uk/20110130111510/http:/schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734>

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it can not be accessed by anyone who does not:

• have permission to access that data, and/or

• need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office, for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

38

The DPA lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

Guidance for organisations processing personal data is available on the Information Commissioner’s Office website: <https://ico.org.uk/for-organisations/>

**Policy and practise**

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (see Privacy Notice section below)

**Personal Data**

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

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

**Responsibilities**

The school’s Senior Information Risk Officer (SIRO) is *Mrs Hilary Tyreman.* This person will keep up to date with current legislation and guidance and will:

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

The school will identify Information Asset Owners (IAOs) *for the various types of* data being held (e.g. pupil / student information / staff information / assessment data etc). 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 has been amended or added to over time
* who has access to protected data and why.

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

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

39

**Registration**

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner-Information to Parents / Carers – the “Privacy Notice”

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils of the data they collect, process and hold on the pupils., 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 the school prospectus and specific letter to all parents/carers. Parents/carers of young people who are new to the school will be provided with the privacy notice the school prospectus and specific letter on data held. See examples at end of this policy,

**Training & awareness**

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

• Induction training for new staff

• Staff meetings / briefings / Inset

• Day to day support and guidance from Information Asset Owners

**Risk Assessments**

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

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

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Information Asset affected** | **Information Asset Owner** | **Protective Marking (Impact Level)** | **Likelihood** | **Overall risk level (low, medium, high)** | **Action(s) to minimise risk** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Impact Levels and protective marking**

Following incidents involving loss of data, the Government published *HMG Security Policy Framework* <http://www.cabinetoffice.gov.uk/spf> , which recommends that the Government Protective Marking Scheme is used to indicate the sensitivity of data.

The scheme is made up of five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. The Protective Marking Scheme is mapped to Impact Levels as follows:

|  |  |
| --- | --- |
| **Government Protective Marking Scheme label** | **Impact Level (IL)** |
| NOT PROTECTIVELY MARKED | 0 |
| PROTECT | 1 or 2 |
| RESTRICTED | 3 |
| CONFIDENTIAL | 4 |
| HIGHLY CONFIDENTIAL | 5 |
| TOP SECRET | 6 |

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered ‘unclassified’. The term ‘UNCLASSIFIED’ or ‘NON‘ or ‘NOT PROTECTIVELY MARKED’ may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone’s reputation has a higher impact than damage that might cause short-term embarrassment.

40

Release and destruction markings should be shown in the footer eg. “Securely delete or shred this information when you have finished using it”.

The school will follow the LA guidelines determining HR records etc.

**Secure Storage of and access to data**

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.

* All users will use strong passwords which must be changed each month
* User passwords must never be shared.

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.

41

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) Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

* On the school system personal data will be held in an encrypted file.

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

• the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and

• 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.

Data storage is permitted and removal encrypted media is allowed.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

All paper based Protected and Restricted (or higher) material must be held in lockable storage.

St Mary’s C of E School recognises that under Section 7 of the DPA, <http://www.legislation.gov.uk/ukpga/1998/29/section/7> data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place (see Data protection policy) to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Personal data held in paper form MUST be kept in a secure locked cabinet. This included SENDI records, Safeguarding records and employment records.

**Secure transfer of data and access out of school**

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

• Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location

• Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.;

• When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.

• If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.

• Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

• Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event. (nb. to carry encrypted material is illegal in some countries)

42

**Disposal of data**

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log is kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation

**Audit Logging / Reporting / Incident Handling**

It is good practice, as recommended in the “Data Handling Procedures in Government” document that  the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals. (Mrs Hilary Tyreman – head teacher )

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes: )

• a “responsible person” for each incident;

• a communications plan, including escalation procedures;

• and results in a plan of action for rapid resolution; and

• a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner’s Office based upon the local incident handling policy and communication plan.

**Use of technologies and Protective Marking**

43

The following provides a useful guide:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **The information** | **The technology** | **Notes on Protect Markings (Impact Level)** |
| **School life and events** | School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events | Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services | Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |
| **Learning and achievement** | Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child’s learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs. | Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent. | Most of this information will fall into the PROTECT (Impact Level 2) category.  There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way. |
| **Messages and alerts** | Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means. | Email and text messaging are commonly used by schools to contact and keep parents informed.  Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via “dashboards” of information, or be used to provide further detail and context. | Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information.  General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |

**PRIVACY NOTICE**

***Children in Need or looked after by the Local Authority***

**Privacy Notice - Data Protection Act 1998**

We [***Cornwall County Council***] hold personal data about our children in care or those children to whom we provide services, and use this data to:

* Support children and monitor their progress;
* Provide appropriate support and pastoral care; and
* Assess how well the Local Authority (LA) as awhole is doing.

This information includes personal characteristics and details for the services we provide.

We are required to pass on some of this information (but not the names of individual children) to the Department for Education (DfE) who use it to help with their policy development, LA performance management and funding and to assist with the development of good practice.

If you want to see a copy of the information we hold and share about you then please contact, Mrs. H Tyreman.

If you require more information about how the LA and/or DfE store and use this data please go to the following websites

* <http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause>
* If you are unable to access these websites, please contact the LA or DfE as follows:
* Public Communications Unit  
  Department for Education  
  Sanctuary Buildings  
  Great Smith Street  
  London  
  SW1P 3BT  
  Website: [www.education.gov.uk](http://www.education.gov.uk)

email: [info@education.gsi.gov.uk](mailto:info@education.gsi.gov.uk%20)

Telephone: 0870 000 2288

**PRIVACY NOTICE**

***School Workforce: those employed or otherwise engaged to work at a school or the Local Authority***

**Privacy Notice - Data Protection Act 1998**

We at [**St Marys C of E Primary School in the Local Authority of Cornwall C.C**] are the Data Controller for the purposes of the Data Protection Act.

Personal data is held by the school about those employed or otherwise engaged to work at the school or Local Authority. This is to assist in the smooth running of the school and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

* Improving the management of school workforce data across the sector;
* Enabling a comprehensive picture of the workforce and how it is deployed to be built up;
* Informing the development of recruitment and retention policies;
* Allowing better financial modeling and planning;
* Enabling ethnicity and disability monitoring; and
* Supporting the work of the School Teacher Review Body and the School Support Staff Negotiating Body.

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

***We will not give information about you to anyone outside the school or Local Authority (LA) without your consent unless the law and our rules allow us to.***

We are required by law to pass on some of this data to:

* the LA
* the Department for Education (DfE)

If you require more information about how the LA and/or DfE store and use this data please go to the following websites:

* <http://www.education.gov.uk/schools/adminandfinance/schooladmin/a0077963/what-the-department-does-with-school-workforce-data>

If you are unable to access these websites, please contact the LA or DfE as follows:

* Public Communications Unit  
  Department for Education  
  Sanctuary Buildings  
  Great Smith Street  
  London  
  SW1P 3BT

Website: [www.education.gov.uk](http://www.education.gov.uk)

Email: [info@education.gsi.gov.uk](mailto:info@education.gsi.gov.uk%20)

Telephone: 0370 000 2288.

**PRIVACY NOTICE TEMPLATE**

**For *Pupils in Schools, Alternative Provision and Pupil Referral Units***

***and Children in Early Years Settings***

**(This is suggested text which can be amended to suit local needs and circumstances)**

**Privacy Notice - Data Protection Act 1998**

We **at** [**St Marys C of E Primary School in the Local Authority of Cornwall C.C**] are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

* Support your teaching and learning;
* Monitor and report on your progress;
* Provide appropriate pastoral care, and
* Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information**[[1]](#footnote-1)** and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

***We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.***

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

If you want to see a copy of the information about you that we hold and/or share, please contact **Mrs H.Tyreman.**

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

[**https://www.cornwall.gov.uk/council-and-democracy/data-protection-and-freedom-of-information/**](https://www.cornwall.gov.uk/council-and-democracy/data-protection-and-freedom-of-information/)

[**http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause**](http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause)

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

* Cornwall Council, County Hall,Treyew Road,  Truro. TR1 3AY
* Public Communications Unit  
  Department for Education  
  Sanctuary Buildings  
  Great Smith Street  
  London  
  SW1P 3BT

Website: [www.education.gov.uk](http://www.education.gov.uk)

email: <http://www.education.gov.uk/help/contactus>   
Telephone: 0370 000 2288

1. Attendance information is not collected as part of the Censuses for the Department for Education for the following pupils / children - those aged under 4 years in Maintained schools and those in Alternative Provision and Early Years Settings. This footnote can be removed where Local Authorities collect such attendance information for their own specific purposes. [↑](#footnote-ref-1)