"I am the way, the truth, and the life." (John 14:6)

St Mary's is a Catholic Primary School.
We place our children at the heart of all we do,
Inspired by the love, life and teachings of Jesus
And the Catholic Christian Church

Data Protection Procedures

These procedures apply to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and Guidance

These procedures meet the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.
In addition, these procedures comply with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. All our procedures are in line with the funding agreement and articles of association of Plymouth CAST.

Data Protection Co-ordinator

Our named data protection co-ordinator is Carol Pipkin, school administrator. Her role is supported by Susan Buscombe, ICT Lead and Jacqui Scarborough, Head-Teacher. As a team they are responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

Data Controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Plymouth CAST, on behalf of the school, is registered as a data controller with the ICO and will renew this registration every five years, as legally required.

Privacy Notices

We have two privacy notices relevant to our school which are available to view on the school website. The privacy notice for parents outlines how we process pupil data and is displayed in the school Reception area and in the showcase in the entrance to the Reception playground. The privacy notice for school staff is displayed in the staff room.

GDPRIS

We use an electronic system for mapping of information sources, both our suppliers and our internal data systems. Any data breaches should be recorded electronically using this system. All staff and governors have been provided with a login to this system and are expected to record any data protection breaches. The decision whether to report a data breach to the ICO will be taken by the data protection co-ordinator in conjunction with the Head Teacher.

Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.
When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the attainment of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

Visitors

All visitors are asked to sign in on arrival to the school. The visitor book will not allow the personal information of other visitors to be viewed. To maintain confidentiality, the glass screen is only opened as necessary by the office staff. Visitors who wish to speak privately are given this option by the office staff, as indicated by a sign on the glass screen.

Clear Screen Policy

In order to preserve the confidentiality of data held in school it is our policy that all members of staff should lock their PC screens when leaving it unattended. This can be achieved by pressing the CTRL+ALT+Delete keys simultaneously and then selecting the lock option. When talking to parents, professionals or other members of staff who do not need access to the data the screen should be positioned so that it cannot be viewed or locked.

Encryption

All laptops that are taken off site are encrypted using the Bitlocker software. This software is tested monthly during the NCi support visits. If a laptop was to be mislaid or stolen this breach should be reported immediately to NCi via the support address help@ncitech.co.uk It should also be reported as a breach to the data protection co-ordinator and ICT lead.

Passwords and Passcodes

All staff are issued with network and email passwords. Teaching staff also have passwords for SIMS, Target Tracker and relevant online or cloud based software. It is essential that passwords are not shared. It is not considered good practice to write down passwords, however should this be deemed necessary this information should be locked away securely when not in use.

Passwords should be at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals

Teaching staff and governors have been provided with an iPad. Every iPad must be secured using a 6 figure passcode. Ipads are supervised using the Profile Manager software on the Mac Server. Ipads can be tracked and traced using the Apple software. If an iPad was lost or stolen it should be reported to the ICT lead and/or NCi via the support email help@ncitech.co.uk
Pupil iPads may also contain personal data and as such it is the responsibility of the class teacher to ensure that all iPads are kept securely when not in use. At the end of the day pupil iPads must be locked away securely.

Governance

As a governing body we are paperless and each governor has been given an iPad, where they do not have their own Apple device. Governors may use their own iPad when following the protocols set out in these procedures. School provided iPads must be supervised and linked to the school iTunes account. All ipads must have a 6 figure passcode. Each governor will be provided with a school email address and correspondence will only be sent to this email address. Documents for governing body meetings should be saved into the 'Good Reader' app and may also be saved in the 'One Drive' encrypted cloud storage area linked to their school email address. If a school provided iPad is lost or stolen it should be reported to the ICT lead and/or the Head Teacher as soon as possible. Where a governor is using their own iPad and it is lost or stolen this should be reported to the data protection co-ordinator as a matter of urgency. If a governor considers that confidential data has been compromised it should be reported to the Data Protection Co-ordinator and/or the Head Teacher as a matter of urgency.

Removable Media

We have made the decision that removable media such as USB sticks must not be used by staff. Staff should save work into the Office 365 'One Drive' folder linked to their email account. Within this account members of staff can choose whether this is a personal document or whether it is to be shared with other members of the school

staff. Documents that are saved within One Drive can be sent electronically as a link or as an attached copy.

Emails

As a school we use Office 365 as our email system. All school correspondence will only be emailed to school provided email addresses, both for staff and governors. Passwords for emails must be kept securely. When emailing personal data about a child or member of staff initials should be used, as appropriate. Documents containing personal data should be password protected and the password for the document sent in a separate email.

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error. Members of staff who receive personal data sent in error must alert the sender and the Data Protection Co-ordinator as soon as they become aware of the error. If the sender is unavailable or cannot recall the email for any reason, the Data Protection Co-ordinator will ask the ICT Lead/NCi to recall it. In any cases where the recall is unsuccessful, the Data Protection Co-ordinator will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way. The Data Protection Co-ordinator will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request. The Data Protection Co-ordinator will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Photographs and Video

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Written consent will include a signature for each aspect of content.

Uses include:

Within school on notice boards and in school magazines, brochures, newsletters, etc.

Outside of school by external agencies such as the school photographer, newspapers, campaigns

Online on our school website and Facebook pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Personal Dated Comments

We keep personal dated comments to record significant incidents and conversations with parents. All comments should only relate to named child. These must be locked away securely at the end of the day in the class stock cupboard.

Accident Forms and Medical Information

The accident forms on the clipboard used to record first aid during the day will be stored in the medical room at the end of the day.
Allergy information for the information of the kitchen staff will be stored in a folder and not on display in the kitchen.
Medical information relating to individual children will be stored on the register alerts. These are stored securely in the school office during the school day. Medical information and care plans kept in the medical room will be kept in a locked cupboard.

Children's Books and Work

During Parent Consultation Meetings children's work is available for parents to view in the classrooms. Parents will be reminded via letter and notices that they should only view the work belonging to their child.
When the school is open to visitors such as during FOSMS events children's books should be stored securely away from public view.
We recognise that there will be times when class teachers may take children's work offsite. During these times the class teacher is responsible for the personal data and should not leave it unattended in a public place.

Data Storage and Security

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of records

Personal data that is no longer needed will be disposed of securely, in line with our retention policies. A copy of our retention policy is available to view in the school office. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
We will shred paper-based records, and overwrite or delete electronic files.

Training

Data protection will form part of continuing professional development for all staff and governors, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring

These procedures will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

Procedures agreed May 2018

Appendix 1.

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Co-ordinator
- The breach should be reported using the GDPRIS system
- The Data Protection Co-ordinator will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Data Protection Co-ordinator will alert the headteacher and the chair of governors
- The Data Protection Co-ordinator will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The Data Protection Co-ordinator will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Data Protection Co-ordinator in conjunction with the Headteacher will work out whether the breach must be reported to the ICO. This must be

judged on a case-by-case basis. To decide, they will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The Data Protection Co-ordinator will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the GDPRIS database.
- Where the ICO must be notified, the Data Protection Co-ordinator will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the Data Protection Co-ordinator will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Data Protection Co-ordinator expects to have further information. The DPO will submit the remaining information as soon as possible
- The Data Protection Co-ordinator will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - The name and contact details of the Data Protection Co-ordinator
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Data Protection Co-ordinator will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Data Protection Co-ordinator will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the GDPRIS software
The Data Protection Co-ordinator and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Appendix 2-Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

	• Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.