St Mary's C of E school
LEARNING WITH HOPE

Data Protection Policy

Organisation name: St. Marys CE VA School

An Baya
TOGETHER WE CAN MAKE A DIFFERENCE

Policy definitions

'We/Us'

- The school named in this policy document

'Data controller'

- The school named in this policy document

'You'

- The person whose data is stored/processed by us

'Data subject'

- The person whose data is stored/processed by us

'Personal data'

- Any information relating to an identified or identifiable living individual

'Special categories'

- Personal data of a sensitive nature and thus subject to a greater level of protection and control, including:
    - Racial or ethnic origin
    - Political views
    - Religious background and beliefs
    - Membership of trade unions
    - Biometric data (e.g. fingerprints)
    - Health information
    - Sexual orientation or sex life

'Data processor'

- A person or professional body other than us who processes data on our behalf

'Processing'

- Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be manual or automated.

'Personal data breach'

- A breach resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

'ICO'

- The Information Commissioner's Office is a non-departmental public body, sponsored by The Department for Digital, Culture, Media & Sport

Policy overview

This policy applies to all personal data (both physical and electronic) processed by us and is designed to ensure that all usage is fair and legal in line with the Data Protection Act 2018 (DPA 2018) and General Data Protection Regulation (GDPR). We have based this document on guidance published by The Information Commissioner's Office (ICO) and their code of practice for subject access requests.[1]

[1] https://ico.org.uk/media/for-organisations/documents/2259722/subject-access-code-of-practice.pdf

Data Controller

We process personal data relating to pupils, parents/carers, job applicants, staff, our governing body, visitors and are therefore defined as a Data Controller.

As a Data Controller, we are registered with the ICO for the purposes of processing personal data.

Roles and responsibilities

This policy applies to all staff, external organisations and other individuals engaged to work on our behalf. Failure to follow this policy in full may result in disciplinary action.

Board of Governors

The Board of Governors has overall responsibility to ensure that we are compliant with all relevant obligations with regard to data protection and GDPR.

Data Protection Officer (DPO)

The DPO is the first point of contact for data-protection-related issues from the ICO. The DPO is responsible for overseeing the implementation of this policy, monitors compliance with data protection laws and is responsible for developing and publishing related policies and guidelines.

The DPO will provide an annual report to the Board of Governors containing related activities, together with a report of any recommendations relating to data protection issues.

Full details of the DPO's responsibilities are set out in the role description.
Our DPO is Glyn Pascoe and is contactable via dpo@ict4.co.uk.

Headteacher

The Headteacher acts as the representative of the Data Controller.

Data Protection Representatives (DPRs)

Data Protection Representatives work closely with the DPO. The DPRs are the first point of contact for individuals whose data the St Mary's School processes. Below is the name of our DPR.

Hilary Tyreman head@st-marys-ce-pz.cornwall.sch.uk

Full details of the DPRs' responsibilities are set out in the role description.

Staff

Staff are responsible for:

- collecting, storing and processing data in accordance with this policy;
- informing the school of any changes to their personal data;
- contacting the DPO if they:
    - have any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - have any concerns that this policy is not being followed.
    - are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
    - feel there has been a data breach.
    - are engaging in a new activity that may affect the privacy rights of individuals.
    - need help with any contracts or sharing personal data with third parties.

Data protection principles

GDPR principles state that personal data must be:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes.
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- accurate and kept up to date where necessary.
- kept for no longer than is necessary for the purpose for which it is being processed.
- processed in a way that ensures it is appropriately secure.

Collecting personal data

Lawfulness, fairness and transparency

By law, there are six legal reasons to process personal data, we will only process personal data under one of these lawful bases:

- To fulfil a contract
- To comply with a legal obligation
- To protect the vital interests of an individual
- To perform a task in the public interest
- To act in the legitimate interests of the organisation
- Where an individual has freely given clear consent

In addition to the above, some of the data we collect is classified as meeting one or more of the special category conditions set out in the GDPR and the Data Protection Act 2018.

We only process special category data when we have both a lawful basis and one of the below conditions for processing as set out in data protection law:

- Explicit consent has been obtained
- Protecting an individual's vital interests in emergency cases where you are physically or legally incapable of giving consent
- The data has already been made public by you
- Processing for legal claims
- Processing it for substantial public interest as defined in legislations
- Processing for health or social care purposes, and the processing is done by or under the direction of a health or social work professional or by another person obliged to confidentially under law
- Processing for public health reasons, and the processing is done by or under the direction of a health professional or by another person obliged to confidentially under law
- Processing for archiving purposes, scientific or historical research purposes or for statistical purposes and the processing is in the public interest.
- Performing an obligation or right in relation to employment, social security or social protection law

Criminal offence data is only processed when we have both a lawful basis and one of the below conditions for processing as set out in data protection law:

- Consent has been obtained
- Protecting an individual's vital interests in emergency cases where you are physically or legally incapable of giving consent
- The data has already been made public by you
- Processing it for or in connection with legal proceedings, to obtain legal advice or exercise or defence of establishment legal rights
- Processing for reasons of substantial public interest as defined in legislation

Limitation, minimisation and accuracy

Data is only collected for specified, explicit, legitimate reasons. These reasons will be communicated to the data subject when their data is collected.

Should we wish to use the data for a reason other than that originally given, we will inform the data subject, requesting consent where necessary.

Staff must only process personal data in order to discharge their duties as part of their role and must ensure that data is deleted or anonymised when it is no longer needed. This will be performed in accordance with the Information and Records Management Society's 'Toolkit for Schools', 2019 being the latest version at going to print. A copy of which is available here.

Sharing of personal data

Data may be shared with third parties where:

- the safety of our staff or pupils is at risk.
- we need to liaise with other agencies.
- the third party is a supplier or contractor engaged on behalf of the school to deliver a service. To ensure compliance, we will:
    - agree a 'data sharing agreement' with the third party.
    - seek to appoint contractors who can confirm that they process data in line with data protection law.
    - share only the data that the third party needs to carry out their service.

Data will also be shared with law enforcement, regulatory and government bodies where legal to do so, examples include:

- To aid the prevention or detection of a crime
- To assist with the prosecution of offenders
- In association with the HRMC for the collection of tax
- In connection with any other legal proceedings
- To comply with our safeguarding obligations
- For research or statistical purposes, either as anonymised data or where consent has been provided

In an emergency situation, personal data may automatically be shared with emergency services and/or related authorities in order to aid them in responding.

Where data is transferred to a territory outside of the European Economic Area, it will be dealt with in accordance with data protection law in the UK.

Subject access requests and your rights

Subject access requests

All individuals can make a 'subject access request' to view a report of the personal information held about them. This may include:

- A statement confirming whether their data is being processed
- A copy of the data held about them
- An outline of the purposes given for holding/processing the data
- The categories of the data held
- Confirmation of whom the data has been shared with, or may be in the future
- The criteria given for governing how long the data is held for (retention policy)
- The source of the data if gathered from a source other than the data subject

- Whether any automated decision-making has been applied to the data and the consequences of that this might have for the individual
- The safeguards in place if the data is being transferred internationally

Submitting a subject access request

A subject access request must be submitted in writing, either by letter or email addressed to the Data Protection Representative, containing:

- The name of the individual
- A correspondence address
- Contact telephone number and email address
- Details of the information being requested

Where a subject access request is received by any other member of staff, it should immediately be forwarded to the Data Protection Representative.

Subject access requests for children

Regardless of age, a child's personal data belongs to them and not their parents or carers and consent to submit a subject access request must be gained. However, children aged 12 years and under are considered not mature enough to fully understand the implications and concepts of a subject access request. The pupil's ability to understand their rights will be judged by the school on a case-by-case basis prior to proceeding with the subject access request.

Responding to a request

In responding to a request, we:

- will ask the individual to provide two forms of identification in person to the related school.
- will respond within one month of passing the verification checks.
- may contact the individual via phone to confirm the subject access request
- will make no charge for providing the information.
- may request an extension of up to a total of three months where the request is complex in nature, informing the individual of why an extension is required. If this is applicable we will inform the individual within one month, and explain why the extension is necessary.

The request may not include specific information or be granted in the following circumstances:

- If the request may result in serious harm to the physical or mental health of the pupil or another individual.
- If the result or the process would reveal that the pupil is at risk of abuse or has been abused, where the disclosure of this information would not be in the pupil's best interests.
- If the data is contained in adoption or parental order records.

- If the data is provided to a court in legal proceedings related to the pupil concerned.
- If the data is part of sensitive documentation including aspects such as immigration, crime, legal proceedings, negotiations, confidential references or exam results.
- If the data contains other identifiable data subjects that cannot easily be redacted or anonymised.

A reasonable fee may be charged where a request is considered excessive or unfounded and we may refuse to action it. A request is considered excessive and/or unfounded where it contains a repeat of information already supplied.

Refusing a request

Where a request is refused, we will inform the individual of the reasons and that they have the right to complain to the ICO. They will also be informed they can seek to enforce their subject access rights through the courts.

Other data protection rights

Individuals have the right to receive information when we are collecting data relating to how we plan to use and process it. Individuals also have the right to:

- Withdraw consent to processing at any time
- Asking to rectify, delete or restrict processing of their personal data or object to the processing (in certain circumstances)
- Prevent the use of personal data for direct marketing purposes
- Challenge the definition of 'public interest' as a basis for processing data
- Challenge decisions based purely on automated decision-making (by computer system)
- Be notified should a data breach occur (in certain circumstances)
- File a complaint with the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals must submit any request relating to the above directly to the DPR who will liaise with the DPO in order to respond.

Educational record

Parents/carers with parental responsibility have a legal right to free access to their child's educational record, which typically includes the most information about a pupil. This can be provided within 15 school days following receipt of a written request.

Photographs and video

Photographs and videos are often recorded, and consent obtained where this is to be used for marketing and promotional materials. We will communicate how the photograph or video will be used, including in some of the potential scenarios below:

- Within the school notice boards, magazines, newsletters
- Online on school blogs, websites or social media
- Outside of school for marketing campaigns, newspapers and other related publications

Should consent be withdraw, we will delete the photograph/video and will not distribute further.

If photographs/media of our pupils are used, they will not be accompanied by any other information, ensuring that pupils cannot be identified.

Photographs and videos taken by parents / carers at school events for their own personal use are not covered by data protection legislation. We will ask that if these images / videos contain pictures of other pupils that they are not shared publicly on social media or other online services for safeguarding reasons. Parents / carers can seek consent from the other parents / carers to use the images / videos on social media.

Our self-published Child Protection (CP) Policy, Photography Policy and Safeguarding Policy contain further information relating to the use and control of photographs/videos taken and distributed by the school.

Data protection by design and default

In line with recommendations from the ICO:[2]

- We consider data protection issues as part of the design and implementation of systems, services, products and business practices.
- We make data protection an essential component of the core functionality of our processing systems and services.
- We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.
- We only process the personal data that we need for our purposes, and we only use the data for those purposes.
- We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.

[2] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

- We provide the identity and contact information of those responsible for data protection within our organisation.
- We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.
- We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.
- We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.
- We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.
- When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.
- Conducting regular external audits of our processes and procedures.
- Maintaining a data asset log, listing aspect such as type, location, security, retention, shared with to name but a few.
- We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

Data security and storage of records

Data will be protected to keep it safe from unauthorised or unlawful access, processing, disclosure or damage.

- Paper-based records will be physically protected and will not be left in communal areas such as classrooms or office desks, pinned to noticeboards or left anywhere where there is general access.
- Electronic devices such as laptops and hard drives will be physically secured when not in use.
- In instances where personal information must be removed from site, data must be signed in/out and the DPR must be made aware.
- To access electronic systems, passwords must be at least eight characters long, containing both letters and numbers.
- Encryption software must be used to protect all portable devices such as laptops and USB devices.
- Two factor authentication will be used where systems allow
- Personal devices should not be used for storing school data.
- Due diligence will be undertaken with third parties where a data sharing agreement must exist.

Data destruction and disposal of records

Personal identifiable data that is no longer required will be disposed of securely, for example paper-based records will be shredded or incinerated either by us or a third-party engaged on our behalf subject to sufficient guarantees that they comply with data protection laws.

Electronic files will be deleted and waste IT hardware securely deposed of by a qualified recycler able to provide a certificate of destruction.

Data breaches

As a responsible organisation, we will make reasonable endeavours to avoid a data breach.

Should a data breach take place, the following process will be followed:

- When a data breach is suspected to have occurred the staff member should immediately notify the DPO by completing the "Form for reporting a data breach" in full providing as much information as possible and email to DPO@ict4.co.uk and follow this up with a phone call to 01209 311344.
- The DPO will investigate to identify whether there is reasonable likelihood that a breach has occurred, considering whether personal data has been accidentally or unlawfully:
    - stolen
    - lost
    - destroyed
    - amended with approval
    - disclosed or made available to a third party or the public without approval.
- The DPO will take all reasonable actions to contain and reduce the impact of the breach.
- The DPO will assess the potential consequences of the breach and their likely impact.
- The DPO will consider whether the ICO should be notified of the breach, based on whether it is likely to cause any material or non-material damage, or negatively affect a person's rights and freedoms, through:
    - identity theft
    - fraud
    - financial loss or significant economic disadvantage
    - damage to reputation
    - loss of confidentiality
    - discrimination
    - loss of control over their personal data.
- If the decision is taken to notify the ICO, this will be completed by the DPO within 72 hours, outlining:
    - the contact details of the DPO;
    - a description of the breach, including:
        - approximate numbers of the individuals affected,
        - approximate numbers of personal data records included in the breach,
        - likely consequences;
    - details of the actions taken/to be taken to deal with the breach and mitigate the impact on the affected individuals.

        - Should any of the above details not be fully know, the report will be as complete as can be reasonably expected and contain a target date for when the information will be collated together with the reasons for the delay.
- Alerting will take different routes depending on the breach:
    - Notifiable to the ICO:
        - The DPO will alert the DPR who will then liaise with the board of governors.
        - If for reasons of conflicts of interest or other maters the DPO has the authority to liaise directly with the Headteacher / Chair of Governors.
    - Not notifiable to the ICO:
        - The DPO will alert the DPR and or Headteacher
        - Reporting of these incidents will be via the governors reports.
- The DPO will maintain a detailed record of all breaches. This log will contain ICO recorded breaches and non ICO recorded breaches. The Logs and associated files will be securely stored electronically in Microsoft UK Data Centres by the DPO. The log will include:
        - a statement of the facts surrounding the breach;
        - likely cause;
        - likely effects on the individuals concerned;
        - actions, both those already taken and suggested actions for the future to avoid it happening again.
- For breaches where the projected impact is considered to be high, the DPO will arrange to communicate with the individuals affected, setting out:
    - the contact details of the DPO,
    - an overview of the breach and the likely consequences to the individual,
    - details of the efforts already made to mitigate the impact of the breach and their potential effects on the individuals affected.
    - The DPO will liaise and notify with any relevant third parties – e.g. insurers, financial institutions etc.
    - The DPO will document the breach fully, regardless of whether the breach is declared to the ICO, including:
    - The DPO should meet with the Headteacher to discuss how to avoid a re-occurrence.

Example actions to a specific breach

Outlined below is an example of a common data breach along with our templated response and actions. Only to be viewed as a guide, each breach is treated and reviewed on a case by case basis and certain aspects would be complex to document the relevant steps due to the uniqueness of some occurrences.

1. Data breach via electronic messaging eg email
    1.1. If sensitive information is made available via email, the sender should attempt to recall the email as soon as they are aware of the breach taking place. The action of

recalling a message often does not actually remove the email from the recipients' inbox but it is part of the process of quickly alerting the recipients' that there has been an issue.

1.2. If possible the sender should contact the recipients immediately and request that the email is deleted and request written (email) confirmation that this has been deleted. Where possible screen shots showing the email in the deleted folder and also a screenshot of the "Recover Deleted Items" folder / panel.

1.3. Once the initial damage limitation process has been completed the sender should complete the "Form for reporting a data breach" and inform the DPO via email dpo@ict4.co.uk and follow up with a phone call to 01209 311344 to ensure safe receipt. As much information should be provided including screenshots and any supporting information no matter how trivial.

1.4. The reporting window is extremely small, therefore providing an accurate full account in a timely manner is imperative.

1.5. The DPO will review the information provided and undertake a risk assessment based upon ICO guidance and ascertain if the breach is reportable. The DPO would then follow the reporting a data breach flow process within this document.

Training

All staff and governors are provided with data protection training as part of their induction process. All staff must attend one training/update course per year.

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

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **every year** and shared with the full governing board.