St Mary's Catholic Primary School
DATA BREACH POLICY

July 2018

Version and Date		Action/Notes
1.0	Aug 2018	For approval
1.1		

INTRODUCTION

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

This policy is the governors' response to these requirements and this outlines the standards that the school requires all users of the school's systems and processes to observe, the circumstances in which the school will monitor use of the systems and processes and the action the school will take in respect of any breaches of these standards.

The wording for this policy comes from templates provided by Judicium, Stone King and the Key for School Leaders with additional input from the ICO.

PURPOSE

The GDPR places obligations on staff to report actual or suspected data breaches and the school's procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Breach of this policy will be treated as a disciplinary offence which may result in action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the school and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

Data processors (see definition below) will be provided with a copy of this policy and will be required to notify the Headteacher, School Business Manager and/or the Data Protection Officer (DPO) of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the data processing agreement.

1) DEFINITIONS

Data Breach

The Information Commissioner's Office (ICO) defines a personal data breach broadly as follows: a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Data Processor

Any person or organisation, other than an employee of the school as data controller, who processes data on behalf of the school (e.g. the payroll provider, the HR consultants).

Data Protection Officer (DPO)

The primary role of the Data Protection Officer (DPO) is to ensure that the school processes the personal data of its pupils, parents and carers, staff, governors, providers or any other individuals (also referred to as data subjects) in compliance with the GDPR related regulations.

The details of the school's DPO are as follows: -

Data Protection Officer: Craig Stilwell
Address: 72 Cannon Street, London, EC4N 6AE
Website: www.judiciumeducation.co.uk
Email: dataservices@judicium.com
Telephone: 0203 326 9174

Data Subject

Person to whom the personal data relates.

ICO

ICO is the Information Commissioner's Office.

Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data, but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

2) RESPONSIBILITIES

The Headteacher has overall responsibility for breach notification within the school. The Headteacher is responsible for ensuring breach notification processes are adhered to by all staff and is the designated point of contact for personal data breaches.

In the absence of the Headteacher, a breach (potential or actual) should be referred to the School Business Manager or the DPO.

The DPO is responsible for overseeing this policy and developing data-related policies and guidelines.

The DPO should be contacted with any questions about the operation of this policy or the GDPR or if there are any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below: -

Data Protection Officer: Craig Stilwell
Address: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Telephone: 0203 326 9174

3) SECURITY AND DATA-RELATED POLICIES

Staff should refer to the following policies related to this data protection policy: -

- **CCTV policy** which manages and regulates the school's use of its CCTV system;
- **Electronic Information and Communications policy** which sets out the school's standards required, the circumstances in which the school will monitor use of these systems and the action the school will take in respect of any breaches of these standards;
- **Data Protection and Freedom of Information policy** which sets out the School's obligations under GDPR about how they process personal data.
- **Information Security policy** which sets out the School's guidelines and processes on keeping personal data secure against loss and misuse
- **Photograph policy** which sets out the school's approach to taking and storing photographic and video images;
- **Records Retention policy** which sets out the school's schedule for holding and destroying data.

These policies are designed to protect personal data and can be found at on the shared drive in the school's computer system.

4) DATA BREACH PROCEDURE

4.1 What Is A Personal Data Breach?

A personal data breach is defined above as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

4.2 When Does It Need To Be Reported?

The school must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes, but is not exclusive to the following: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

4.3 Reporting a Data Breach

If a personal data breach is known to have occurred or has been suspected to have occurred or may occur which meets the criteria above, the following procedure should be followed:

- A data breach report form should be completed (which can be obtained from the Headteacher or School Business Manager);
- The completed form should be handed or e-mailed or posted to the Headteacher, the School Business Manager or the Data Protection Officer (with a copy being sent to the Headteacher).

Where appropriate, staff members should liaise with their line managers about completion of the data breach report form. Breach reporting is encouraged throughout the school and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, the Headteacher, School Business Manager or the DPO.

Once reported, the staff member should not take any further action in relation to the breach. The Headteacher, School Business Manager or the DPO will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the ICO.

4.4 Managing and Recording the Breach

Immediate steps must be taken to establish whether a personal data breach has in fact occurred. If so the following steps will be taken:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO;
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

Notification of a suspected data breach will be advised the Chair of Governors or Vice Chair.

4.5 Notifying the ICO

The ICO must be notified when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (I.e. it is not 72 working hours). If the school is unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

4.6 Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Headteacher or, in the Headteacher's absence, the School Business Manager will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the school have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the Headteacher's absence, the School Business Manager will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the school will consider alternative means to make those affected aware (for example by making a statement on the school website).

4.7 Notifying Other Authorities

The School will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers;
- Diocese;
- Trustees;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is not exhaustive.

4.8 Assessing the Breach

Once initial reporting procedures have been carried out, the school will carry out all necessary investigations into the breach.

The school will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. The school will identify ways to recover correct or delete data (for example notifying its insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the school will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected; Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school;
- And, any other wider consequences which may be applicable.

4.9 Preventing Future Breaches

Once the data breach has been dealt with, the school will consider its security processes with the aim of preventing further breaches. In order to do this, the school will undertake the following: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To brief governors following the investigation.

5) REPORTING DATA PROTECTION CONCERNS

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and staff members are encouraged to report any concerns (even if they do not meet the criteria of a data breach) there might be to the Headteacher or the DPO. This can help capture risks as they emerge, protect the school from data breaches and keep our processes up to date and effective.

6) MONITORING

The school will monitor the effectiveness of this and all of our policies and procedures relating to GDPR and conduct a full review and update as appropriate.

The school's monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

This Policy is reviewed by the Resources Committee every two years and must be signed by the Chair of Governors and Headteacher.

Policy Reviewed: Autumn term 2018

Next Review: Autumn term 2020

Signature of Chair of Governors:

Signature of Headteacher: