All Saints Church School
A Bath and Wells Academy

Special Categories of Personal Data Policy

1. Introduction

All Saints Church School issues this policy to meet the requirements incumbent upon them under the General Data Protection Regulations 2016 (GDPR) and the Data Protection Act 2018 for the handling of special categories of personal data in its role as a data controller and data processor.

2. Scope

This policy applies to all employees of All Saints Church School including contract, agency and temporary staff, volunteers, Governors and employees of partner organisations working for All Saints Church School

Special Categories of Personal Data (formerly known as Sensitive Personal Data) requires additional legal basis to process, along with additional protections.

The categories of data within scope of this policy are special categories of personal data revealing:

a) racial or ethnic origin
b) political opinions
c) religious or philosophical beliefs
d) trade union membership
e) genetic data
f) biometric data for the purpose of uniquely identifying a natural person
g) data concerning health; or
h) data concerning a natural person's sex life or sexual orientation

All Saints Church School will set out the types of special categories of personal data it processes on data subjects in its Privacy Notices which are available https://allsaintsprimary.j2bloggy.com/ Or by contacting the Data Protection Officer (i-west@bathnes.gov.uk). It will also include the processing on its Register of Processing Activity (Information Inventory) which is updated annually.

3. Legal Basis

In addition to the legal basis to process personal data under Article 6(1), special categories of personal data will also requires an additional legal basis for processing under Article 9(2). These are:

a) the data subject has given explicit consent to the processing of their personal data for one or more specified purposes

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights under **employment and social security and social protection law**;
c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
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;
e) processing relates to personal data which are **manifestly made public by the data subject**;
f) processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;
g) processing is necessary for reasons of **substantial public interest** but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision making process.

- Statutory and government purposes
- Administration of Justice and parliamentary purposes
- Equality of opportunity or treatment
- Preventing or detecting unlawful acts
- Protecting the public against dishonesty
- Journalism in connection with unlawful act and dishonesty
- Preventing fraud
- Processing for the purposes of preventing fraud.
- Suspicion of terrorist financing and money laundering
- Counselling
- Insurance
- Occupational pensions
- Political parties
- Elected representatives responding to requests
- Disclosure to elected representative
- Informing elected representatives about prisoners
- Publication of legal judgements
- Anti-doping in sport
- Standard of behaviour in sport

h. processing is necessary for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i. processing is necessary for 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 quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4. Roles and Responsibilities

All stakeholders which include staff, contractors, consultants, suppliers, volunteers, governors and trustees must:

a) Be familiar with this policy and other relevant policies and procedures including, but not limited to:
   i. Data Protection Policy
   ii. Special Categories of Personal Data Policy
   iii. Data Breach Policy
   iv. Data Retention Policy (IRMS Toolkit)
b) Play an active role in protecting information in their work
c) Read and act on any training and awareness, and communications regarding information security and ask for clarification if these are not understood
d) Take care when handling information to ensure it is not disclosed to those without the need to know or are not approved
e) Report any breaches, near misses, or incidents to the organisation via the organisation's Data Breach Policy and procedures

Governors and Senior Leaders are required to:

a) Approve this policy
b) Actively promote a culture of privacy and security
c) Ensure security and privacy is considered throughout the development of any new service, process or product
d) Cascade any relevant communications regarding information security
e) Ensure Information Owners and Information Custodians are assigned for its critical information assets

Ultimately this group are accountable for the organisation's information, therefore there may be other elements that this cohort deliver as part of their roles.

Data Protection Officer is required to:

a) Monitor compliance with Data Protection Law and this policy, reporting this to the Local Governing Board annually.
b) Assist the organisation with any Data Protection Impact Assessment which could include recommending controls to reduce risk
c) Assist the organisation with any queries they have regarding data protection

5. Data Protection Impact Assessments (DPIA)

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity All Saints Church School will consult with its Data Protection Officer assess risks based on an initial screening process. The DPIA will:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

Upon completion of a DPIA the regulator (ICO) maintains the right to cease the proposed processing should it remain high risk.

Please refer to the Data Protection Impact Assessment Policy for more details.

6. Additional protections

All Saints Church School will ensure additional protections are applied to Special Categories of Personal Data. These are:

- Data will be kept on an individual's person when taken offsite
- Data will be locked away when not in use
- The following principles will be strongly considered:
    - Data Minimisation
    - Encryption
    - Pseudonymisation

7. Monitoring and compliance

Compliance with this policy shall be monitored through an annual review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the Head Teacher, Local Governing Body and BWMAT Central Team.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with senior management, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

Review this Policy upon;
Change of Data Protection Officer,
Change of Legislatio