Whickham Parochial Church of England Primary School

Data Protection Policy

Updated April 2022

Mission Statement

At our Parochial school we aim to provide a stimulating and caring environment in which every child flourishes, with Christianity at the heart of all we do.

Aims

At Whickham Parochial we believe that every child is entitled to enjoy their childhood, celebrate their individuality and reach their full potential. We aim to do this through:

- Creating a caring school family living by Christian values.
- Celebrating everyone's strengths and efforts.
- Valuing the opportunities we have to contribute to our community and the wider world.
- Offering wide ranging quality experiences that stimulate children's minds.
- Encouraging respect for others, positive behaviour and good manners, enabling all children to feel secure and valued.
- Building strong links between school, home and church.
- Preparing children for future challenges in a changing world

We wish every child to take with them happy memories of Whickham Parochial into their future life.

DATA PROTECTION POLICY

1.0 Introduction

1.1 Whickham Parochial School's Data Protection Policy has been produced to ensure we are compliant with the Data Protection Act 2018 (DPA), GDPR and associated legislation, and it incorporates guidance from the Information Commissioner's Office (ICO).

1.2 The GDPR & the DPA gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

1.3 The School is registered with the ICO as a Data Controller for the processing of living individuals' personal information.

Our data controller registration number is: Z5579137

2.0 Purpose

2.1 The School Data Protection Policy has been produced to ensure it is compliant with the GDPR & DPA 2018.

2.2 The Policy incorporates guidance from the ICO, and outlines the School's overall approach to its responsibilities and individuals' rights under the DPA 2018.

3.0 Scope

3.1 This Policy applies to all Employees & Governors (including temporary, casual or agency staff, contractors, consultants and suppliers working for, or on behalf of the School), third parties and others who may process personal information on behalf of the School.

3.2 The Policy also covers any staff and students who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the relevant School to ensure the data is processed in accordance with the GDPR & DPA 2018 and that students and staff are advised about their responsibilities. In addition, the activity should be referred to the Research Ethics Committee.

4.0 Data covered by the Policy

4.1 A detailed description of this definition is available from the ICO, however briefly, personal data is information relating to an individual where the structure of the data allows the information to be accessed i.e. as part of a

relevant filing system. This includes data held manually and electronically and data compiled, stored or otherwise processed by the School, or by a third party on its behalf.

4.2 Sensitive personal data is personal data consisting of information relating to:

· Racial or ethnic origin

· Political opinions, Religious beliefs or other beliefs of a similar nature

· Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)

· Physical or mental health or condition

· Sexual life or sexual orientation

· Genetic or biometric documentation

5.0 The Six Data Protection Principles

5.1 The GDPR & the DPA 2018 require the School staff , Governors and others who process or use any personal information must comply with the six data protection principles. The School must be able to demonstrate compliance with the law in accordance with GDPR & the DPA accountability principle.

5.2 The principles require that personal data shall:

· Be processed fairly, lawfully and in a transparent manner

· Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose

· Be adequate, relevant and limited to what is necessary in relationship to the purposes for which the data is processed

· Be accurate and kept up to date

· Not be kept for longer than is necessary

· Be kept safe from unauthorised or unlawful processing and against accidental loss, destruction or damage

6.0 Responsibilities

6.1 The School must appoint a Data Protection Officer to handle day-to-day issues which arise, and to provide members of the School with guidance on Data Protection issues to ensure they are aware of their obligations. The duties, tasks and appointment of the DPO are defined in articles 37-39 of the GDPR. Please contact the DPO for schools should you have any concerns, queries or complaints in relation to any aspect of the schools data protection compliance.

Contact details -

Rachel Walton Telephone – 0191 4887867

E-mail – rachelwalton@gateshead.gov.uk

6.2 All new members of staff will be required to complete a mandatory information governance module as part of their induction and existing staff will be requested to undertake refresher training on a regular basis.

6.3 Employees of the School are expected to:

· Familiarise themselves and comply with the six data protection principles

· Ensure the possessing of personal data of pupils, parents, staff and Governors is accurate and up to date

· Ensure their own personal information is accurate and up to date

· Keep personal data for no longer than is necessary

· Ensure that any personal data they process is secure and in compliance with the School's information related policies and strategies. Please contact the School Business Manager

· Acknowledge data subjects' rights (e.g. right of access to all their personal data held by the School) under the GDPR & DPA 2018, and comply with access to records

· Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern the School/Academy

· Obtain consent where necessary when collecting, sharing or disclosing personal data

6.4 Students, of the School are expected to:

· Comply with the six data protection principles

· Comply with any security procedures implemented by the School.

7.0 Obtaining, Disclosing and Sharing

7.1 Only personal data that is necessary for a specific School related business reason should be obtained.

7.2 Students are informed about how their data will be processed when they agree to the Data Processing Consent Notice upon registration.

7.3 Upon acceptance of employment at the School, members of staff also consent to the processing and storage of their data.

7.4 Data must be collected and stored in a secure manner.

7.5 Personal information must not be disclosed to a third party organisation without prior consent of the individual concerned. This also includes information that would confirm whether or not an individual is or has been an applicant, student or employee of the School.

7.6 The School may have a duty to disclose personal information in order to comply with legal or statutory obligation. The GDPR & DPA 2018 allows the disclosure of personal data to

authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function. Any requests to disclose personal data for reasons relating to national security, crime and taxation should be directed to the DPO for schools, see contact details above – paragraph 6.1.

7.7 Personal information that is shared with third parties on a more regular basis shall be carried out under a written agreement/contract, stipulating the purview and boundaries of any information shared. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the GDPR & DPA 2018.

8.0 Retention, Security and Disposal

8.1 Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If an employee, student or applicant is dissatisfied with the accuracy of their personal data, then they must inform the School Business Manager.

8.2 Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with principle 2 and principle 4 of the GDPR & DPA 2018, personal information shall be collected and retained only for business, regulatory or legal purposes.

8.3 In accordance with the provisions of the GDPR & the DPA 2018, all staff whose work involves processing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.

8.4 In accordance with the School's Flexible Working Scheme, staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

8.5 All departments should ensure that data is destroyed in accordance with the Retention Schedule when it is no longer required.

8.6 Personal data in paper format must be shredded or placed in the confidential waste bins provided. Personal data in electronic format should be deleted, and CDs and pen drives that hold personal data passed to your I.T provider for safe disposal. Hardware should be appropriately degaussed/appropriately wiped in compliance with your I.T service provider contract and conforms with DPA and GDPR requirements.

9.0 Transferring Personal Data

9.1 Any transfer of personal data must be done securely in line with the School's Information Security Policy.

9.2 Email communication is not always secure and sending personal data via external email should be avoided unless it is encrypted with a password provided to the recipient by separate means such as via telephone.

9.3 Care should be taken to ensure emails containing personal data are not send to unintended recipients. It is important that emails are addressed correctly and care is taken

when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

9.4 Personal email accounts should not be used to send or receive personal data for work purpose.

10.0 Data Subjects Right

10.1 Under GDPR & the DPA 2018 data subjects have the right of

· Subject access to their personal data held by the School. This applies to data held in both paper and electronic format, and within a relevant filing system.

· The right to erasure/the right to be forgotten, data portability the right to restriction and the right to object.

10.2 The School shall use its discretion under the GDPR & the DPA 2018, to encourage informal access at a local level to a data subject's personal information, but it will also have a formal procedure for the processing of Subject Access Requests.

10.3 Any individual who wishes to exercise their rights should contact the school Business Manager for additional information

10.4 The School may charge a fee in certain circumstances. It will only release any information upon receipt of the completed Subject Access Request Form, along with proof of identity or proof of authorisation where requests are made on the behalf of a data subject by a third party. The requested information will be provided within the statutory timescale of 1 month from receipt of the completed form.

11.0 Reporting a Data Security Breach

11.1 It is important the School responds to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on School systems, and unauthorised use of personal data, accidental loss or equipment failure. Any data breach should be reported to the Head Teacher/School Business Manager in the first instance. The school will notify the Data Protection Officer for further advise and assistance. Please refer to the Data Breach reporting policy for more information.

11.2 Any breach will be investigated in line with the procedures within the Data Breach Policy. In accordance with that policy, the school will treat any breach or security breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.

This policy will be updated in the light of any statutory changes or by May 2025.

R. Walton (Head Teacher)