Goodrich Church of England Primary School

DATA PROTECTION POLICY

Headteacher: Mrs. Karen Miles

Chair of Governors: Mrs. Rose Webb

Policy creation date: May 2018

Last reviewed: May 2019

Policy review date: **May 2020**

1. POLICY STATEMENT

1.1 This is the Data Protection Policy of Goodrich CE Primary School ("The School")

1.2 We are committed to managing personal information carefully and lawfully in accordance with the General Data Protection Regulation ("GDPR") and other related legislation which protects personal information. We recognise the importance of this, and have updated our policy to ensure that it gives effect to important changes in the law introduced by the GDPR.

1.3 During the course of our activities, we will collect, store and process personal data about our staff, pupils and parent(s) / guardian(s) and other individuals who come into contact with the school. We recognise that the correct and lawful treatment of this personal information is critical to maintaining the confidence of those connected with our school, whether that be pupils, parent(s)/guardian(s) or otherwise.

1.4 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 The types of personal data that we may be required to handle includes information about current, past and prospective pupils, staff, parent(s) / guardian(s) and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the GDPR and other regulations.

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy has been approved by the Governing Body. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 The Data Protection Officer (DPO) is responsible for ensuring compliance with the GDPR and related data protection regulations and with this policy. This role will be carried out by the school administrator. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** means an identified or identifiable natural person.

3.3 **Personal data** means any information relating to an identified or identifiable natural person ('data subject').

3.4 **Data controllers** are the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; they are responsible for establishing practices and policies in line with the GDPR. We are the data controller of all personal data used in our school for our own educational purposes.

3.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the school.

3.7 **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise.

3.8 **Special category of personal data** means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. This type of personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned (sensitive personal data).

4. DATA PROTECTION PRINCIPLES

4.1 Anyone processing personal data must comply with the enforceable principles of good practice. These provide that personal data must be:

(a) Processed lawfully, fairly and in a transparent manner.

(b) Collected for specified, explicit and legitimate purposes and not processed further in a way which is incompatible with those purposes.

(c) Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Secure.

5. FAIR AND LAWFUL PROCESSING

5.1 The GDPR is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, it must be processed on the basis of one of the lawful grounds set out under the GDPR. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract to which the data subject is a party, for compliance with a legal obligation to which the data controller is subject, the processing is necessary to protect the vital interests of the data subject, or the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

5.3 When sensitive personal data is being processed (now known as "special categories of personal data" under the GDPR), additional conditions must be met. When we process sensitive personal data, we will ensure compliance with these requirements.

6. PROCESSING FOR LIMITED PURPOSES

6.1 We will only collect and process personal data for specified, explicit and legitimate reasons. We will not further process that personal data unless the reason for doing so is compatible with the purpose or purposes for which it was originally collected.

7. NOTIFYING DATA SUBJECTS

7.1 If we collect personal data directly from data subjects, we will provide information which they are entitled to receive under the GDPR. This will, amongst other things, include the following:-

(a) The purpose or purposes for which we intend to process personal data.

(b) The legal basis on which we believe the processing to be lawful.

(c) The types of third parties, if any, with which we will share or to which we will disclose personal data.

(d) The identity of the school's designated Data Protection Officer.

(e) Their individual rights as set out under the GDPR.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with information required under the GDPR which includes, amongst other things, the identity and contact details of the controller, the purpose and legal basis for the processing, the category of personal data concerned and who that data is shared with.

7.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

8. ADEQUATE, RELEVANT AND LIMITED PROCESSING

8.1 We will only collect personal data to the extent that it is necessary for the specific purpose notified to the data subject.

9. ACCURATE DATA

9.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

9.2 We will take all reasonable steps to ensure that personal information that is inaccurate is either erased or rectified without delay.

10. TIMELY PROCESSING

10.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy and erase from our systems, all data which is no longer required.

11. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

11.1 We will process all personal data in line with data subjects' rights under the GDPR and related laws, in particular their right to:

(a) Request access to any data held about them by a data controller.

(b) Rectification of inaccurate information.

(c) Erasure of personal data concerning the data subject.

(d) Restrict the processing of the data subject's personal data.

(e) Object to the processing of the data subject's personal data.

(f) To receive personal data concerning the data subject in a commonly used format (known as data portability) and have this transferred to another controller without hindrance.

12. DATA SECURITY

12.1 We will take appropriate security measures that ensure appropriate security of personal data, including protection against unlawful or unauthorised processing of personal data, and against the accidental loss of, destruction or damage to, personal data.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if that processor provides a suitable guarantee that it will comply with the GDPR.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

12.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential).

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

13.1 We may share personal data we hold about our pupils and staff in accordance with the GDPR. Where we share personal information we will do this, in most cases, to comply with a legal obligation. Where this is not the case we will, in most other cases, obtain consent first.

13.2 Where we do disclose or share personal information, then we will inform you about this in accordance with this policy.

13.3 Examples of who we may share personal information with include other schools, the local authority or the Department of Education.

14. DEALING WITH SUBJECT ACCESS REQUESTS

14.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward this to the DPO immediately.

14.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

14.3 Our employees will refer a request to the DPO for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

14.4 On receipt of a subject access request, we will send a letter to the requester acknowledging receipt.

14.5 We will respond to subject access requests as soon as possible, but in any event no later than 1 month from the receipt of the request subject to 14.6.

14.6 If the nature of the request is complex, or there are other legitimate reasons for doing so, we may, if necessary, extend the period under 14.5 for up to 2 months. If we require an extension of time of over 1 month to deal with a subject access request, we will inform the requester as soon as possible, but in any event no later than 1 month from the date that the request was made.

14.7 We will not charge a fee for responding to subject access requests unless the request, in the opinion of the school, is unfounded, excessive and/or repetitive.

15. DATA BREACHES

15.1 All data breaches should be immediately reported to the DPO.

15.2 All data breaches must be handled in accordance with the school's internal breach reporting procedure.

16. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time and notification of any changes will be communicated accordingly.