Carbeile Junior School

PRIVACY STANDARD

CONTENTS

1. **DEFINITIONS**

The following definitions apply in this policy:

PO	Privacy Officer
Personal Data	data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller, and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual
Data Subject	a living individual who is the subject of Personal Data
Data Controller	a person (usually an organisation) who (alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data is, or is to be, processed. However, two or more persons (usually organisations) can be joint Data Controllers where they act together to decide the purpose and manner of any data processing. The term “in common” applies where two or more persons share a pool of Personal Data that they process independently of each other
Data Processor	in relation to Personal Data, any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller
ICO	Information Commissioners Office
GDPR	General Data Protection Regulation
School	Carbeile Junior School
Employees	All employees, officers, consultants, contractors, volunteers, interns, casual workers, and agency workers of the School

2. **PURPOSE**

2.1 This Policy sets out how the School complies with the GDPR.

2.2 The importance of keeping clients’ affairs confidential, protecting Personal Data and special personal data and keeping information secure is fundamental. This Policy is designed to ensure that all Employees comply with their obligations to protect data and ensure confidential information is kept confidential.

2.3 This policy covers all Employees but does not form part of any Employee's contract of employment and we may amend it at any time.

3. **RESPONSIBILITY**

3.1 All Employees must familiarise themselves and comply with this Policy and related procedures. Failure to comply with this Policy and the related procedures will result in disciplinary action because of the significant risks of fines and enforcement action, reputational consequences against the School.

3.2 All Employees are responsible for ensuring that all types of data they process are properly protected. Any issues or concerns about the GDPR must be raised with the PO.

4. PRINCIPLES

4.1 The GDPR establishes a framework of rights and duties designed to protect Personal Data. The GDPR requires that Personal Data is processed in compliance with the GDPR principles and individuals rights.

4.2 Article 5 of the GDPR requires that Personal Data is:

4.2.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

4.2.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

4.2.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4.2.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

4.2.5 kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

4.2.6 processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4.3 The GDPR provides the following rights for individuals:

4.3.1 **To be informed** - This encompasses your obligation to provide ‘fair processing information’, typically through a privacy notice. It emphasises the need for transparency over how you use Personal Data.

4.3.2 **Access** - Individuals have the right to access their Personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

4.3.3 **Rectification** - The GDPR gives individuals the right to have Personal data rectified. Personal Data can be rectified if it is inaccurate or incomplete.

4.3.4 **Erasure** - The GDPR gives individuals the right to have Personal Data rectified. Personal Data can be rectified if it is inaccurate or incomplete.

4.3.5 **Restrict processing** - Individuals have a right to 'block' or suppress processing of Personal Data.

When processing is restricted, you are permitted to store the Personal Data, but not further process it.

You can retain just enough information about the individual to ensure that the restriction is respected in future.

4.3.6 **Data portability** - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows individuals to move, copy or transfer Personal Data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

4.3.7 **Object** - Processing based on legitimate interests or direct marketing (including profiling and statistics).

4.3.8 **In relation to automated decision making and profiling** – We do not use automatic decision making or profiling.

4.4 Employees should be aware that under the Computer Misuse Act 1990, there are three criminal offences:

4.4.1 Unauthorised access to computer material;

4.4.2 Unauthorised access with intent to commit or facilitate the commission of further offences; and / or

4.4.3 Unauthorised modification of computer material.

4.5 Employees who are unsure as to whether they are able to access or modify material must contact the PO for guidance. Any commission of or attempt to commit a criminal offence by an employee will be dealt with in accordance with the Disciplinary Procedure.

4.6 All employees must keep Personal Data and information about the School secure at all times. If an employee is concerned that data or confidential information is at risk, he or she must immediately contact the PO.

5. DATA SUBJECTS RIGHTS

5.1 Data subjects have rights when it comes to how we handle their Personal Data. These include rights to:

5.1.1 Withdraw consent to processing at any time;

5.1.2 Receive certain information about the Data Controller's processing activities;

5.1.3 Request access to their Personal Data that we hold;

5.1.4 Prevent our use of their Personal Data for direct marketing purposes;

5.1.5 Ask us to erase Personal Data if it is no longer necessary in relation to the purpose for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

5.1.6 Restrict processing in specific circumstances;

5.1.7 Challenge processing which has been justified on the basis of our legitimate interests;

5.1.8 Request a copy of an agreement under which Personal Data is transferred outside of the EEA;

5.1.9 Object to decisions based solely on automated processing, including profiling;

5.1.10 Prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;

5.1.11 Be notified of a Personal Data breach which is likely to result in high risk to their rights and freedoms;

5.1.12 Make a complaint to the supervisory authority; and

5.1.13 In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

5.2 If a request is made quoting any legislation including but not limited to the GDPR, or references the ICO or the PO, or if an individual makes a clear request, that request must be referred to the PO immediately. Individuals may also ask for details of information held about them without mentioning the word data or the data protection legislation; all such requests must be forwarded immediately to the PO.

5.3 There are strict timescales for compliance with an access request and failure to comply can result in a significant fine from the ICO. Employees must comply with the Breach and Escalation Procedure.

6. ACCURACY OF DATA

Employees must ensure that data is as accurate as possible; if data is or appears to be inaccurate, misleading or not up to date, employees must take reasonable steps to amend / update the information as soon as possible. Data only needs to be kept up to date where necessary and employees should seek guidance if they are not sure whether the data needs to be updated. Any concerns must be discussed with the PO.

7. RETENTION AND DESTRUCTION OF DATA

Personal Data must be retained or disposed of securely in accordance with the School's Data Retention Policy.

8. DATA CONTROLLERS / PROCESSORS

8.1 Personal Data must not be disclosed to another party unless they are a Data Controller or a Data Processor (as defined by this Policy), [and] it is for the purposes of the case. The client must always be advised to whom the data will be disclosed and why.

8.2 Before sending data to a Data Controller or to a Data Processor, the employee must ensure that proper contractual arrangements are in place to protect the data. Alternatively, the employee must contact the PO to determine whether there is already a contractual arrangement or what further steps need to be taken.

8.3 The organisation must ensure that the Data Controller or Data Processor is clear as to the basis on which they will hold the data, when they will return it, what the security arrangements are and what will happen if there is any data loss.

8.4 The PO is responsible for ensuring that appropriate due diligence is undertaken. If an employee has any queries about the way in which a Data Controller or Data Processor is dealing with data, he or she must contact the PO.

Next Review: May 2019

Signed Headteacher: Mr P Hamlyn

Signed Chair of Governors: Mrs. S Morton

Date: 21.05.18