Data Protection Policy

Bridgewater's Data Protection Officer

Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

schoolsDPO@veritau.co.uk
01609 53 2526

Introduction

Bridgewater recognises and accepts its responsibility as set out in the Data Protection Act 2018 (the Act). The School, as a data controller, will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information.

This policy statement applies to all Bridgewater School governors and employees, and individuals about whom the school processes personal information, as well as other partners and companies with which the school undertakes it business.

Rationale

The School needs to collect and use certain types of personal information about people with whom it deals in order to operate. These include current, past and prospective employees, pupils, suppliers, clients, and others with whom it communicates. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used - whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this in the Act.

We regard the lawful and correct treatment of personal information by the School as very important in order to secure the successful carrying out of operations and the delivery of our services, and to maintaining confidence with those whom we deal. The School will treat personal information lawfully, correctly and in compliance with legislative requirements.

Fair Obtaining and Processing

Bridgewater undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely

recipients of the data and the data subjects' right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

Our privacy notices can be found on our website (www.bridgewater.newcastle.sch.uk/home/useful-links/data-protection/)

Aims and Objectives

The School will, through appropriate management and application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements;
- ensure the quality of information used, including its accuracy and relevancy for the purpose(s) specified;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken: the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, block or erase information which is regarded as erroneous);
- take appropriate technical and organisational security measures to safeguard personal information; and
- ensure that personal information is not transferred abroad without suitable safeguards.

In addition, the School will take steps to ensure that:

- there is someone with specific responsibility for data protection in the organisation;
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so;
- everyone managing and handling personal information is provided with guidance and training;
- anybody wanting to make enquiries about handling personal information knows what to do;
- queries about handling personal information are dealt with in 28 days;
- methods of handling personal information are clearly described;
- an annual review and audit is made of the way personal information is managed;
- methods of handling personal information are annually assessed and evaluated;

- performance of handling personal information is annually assessed and evaluated; and
- it disseminates to employees, information on good practice in respect of handling, using and storing personal information.

Processing Rights of Access Requests

We will deal with simple requests for personal data as business as usual. More complicated requests will be dealt with under our Right of Access procedures.

RARs must be submitted to the School Business Manager.

Provided that there is sufficient information to process the request, an entry will be made in the Right of Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than 28 days from the request date).

Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information is provided.

In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 28 days.

Information Sharing

We may share information with third parties where there is a legal obligation to do so, or there is a relevant public interest, or to enable us to carry out official functions, or where we have consent to do so.

Only authorised and trained staff are allowed to disclosure personal information to a third party

Data and Computer Security

Bridgewater undertakes to ensure security of personal data by the following general methods:

Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

Logical Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by the Governing Body and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The School's security policy is kept in a safe place at all times.

Article 33 of the UK UK GDPR requires data controllers to report breaches of personal data to the Information Commissioner's Officer, and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subject(s). Therefore it is vital that the School has a robust system in place to manage, contain, and report such incidents. The Information Security Incident Management Policy details how the School will handle and manage information security incidents when they arise.

Any queries or concerns about security of data in the school should in the first instance be referred to the Business Manager.

Individual members of staff can be personally liable in law under the terms of the Data Protection Act. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. Breaches of this Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

Monitoring & Review

A copy of this policy statement will be issued to all employees. It will be reviewed periodically, added to, or modified from time to time and may be supplemented in appropriate cases by further statements and procedures relating to the work of the particular groups of workers.

Agreed: October 2022
Date of review: Autumn 2023