Bramcote Hills Primary School

Data Protection Policy

September 2018

"Make the Future Better for All"

School Personal Data Handling –Rationale

The risk of data breaches suffered by organisations and individuals makes the area of personal data protection a current and high profile issue for schools, colleges and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on our systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation
- schools are 'data rich' and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school will want to avoid the criticism and negative publicity that could be generated by any personal data breach
- the school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation
- it is a legal requirement for all schools to have a Data Protection Policy.

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and is accessible not just in school but also from remote locations. The Data Protection laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format.

Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed, following the European Union General Data Protection Regulation (GDPR) announced in 2018. This represented a significant shift in legislation and replaced the Data Protection Act 1998. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'. Given the nature of schools and the personal data required in a variety of forms to operate a school, this means that every school in the UK is required to comply. Guidance for schools is available on the Information Commissioner's Office website including information about the new regulations.

Introduction

Bramcote Hills Primary School and its employees do everything within their power to ensure the safety and security of any material of a personal or sensitive nature, including personal data. It is the responsibility of all members of the school community to take care when handling, using or transferring personal data and that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner's Office. Particularly, all transfer of data is subject to risk of loss or contamination. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the statutory requirements contained in relevant data protection legislation and relevant regulations and guidance from the Local Authority.

Definitions

Data Controller: Any individual or organisation who controls personal data, in this instance the school.

Personal Data: Data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

Sensitive Personal Data: Personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life and criminal activities.

Relevant Filing System: Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible e.g. personnel records.

Data Subject: An individual who is the subject of the personal data, for example, employees and pupils.

Processing: Obtaining, recording or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.

Accessible Records: Any records which are kept by an organisation as part of a statutory duty, e.g. pupil records, , social care records.

Registration

Bramcote Hills Primary School is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Responsibilities

The school has a **Data Protection Officer** (DPO), Sue Hewes. The role of the DPO includes:

- informing the organisation of its obligations under the GDPR
- monitoring the impact and application of policies in relation to personal data
- organising training in aspects of GDPR
- acting as the point of contact for and co-operating with the Information Commissioner's Office (ICO)
- consulting on any new processing of data and carrying out Data Impact Assessments.

The DPO will have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level.

The Data Controller will:

- not give the DPO instructions regarding the performance of tasks
- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- not dismiss or penalise the DPO for performing the tasks required of them.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner. Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Bramcote Hills Primary School follows Records Management Society Retention Guidelines for schools to address risks to data. This document determines:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to the data and why.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. In order to comply with its obligations, Bramcote Hills Primary School undertakes to:

- **Process personal data fairly and lawfully**
  The school will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller; the purposes of the processing; any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.
- **Process the data for the specific and lawful purpose for which it collected that data, and not further process the data in a manner incompatible with this purpose**
  The school will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.
- **Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed**
  The school will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind.
- **Keep personal data accurate and, where necessary, up to date**
  The school will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the school if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the school to ensure that any notification regarding the change is noted and acted on.
- **Only keep personal data for as long as is necessary**
  The school undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements.
- **Process personal data in accordance with the rights of the data subject**
  The school will only process personal data in accordance with individuals' rights.
- **Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data**
  All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.
- **Ensure that no personal data is transferred to a country or a territory outside the European Economic Area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data**.
  The school will not transfer data to such territories without the explicit consent of the individual.

Conditions for Processing

The Data Protection Act 2018 provides a set of conditions to be satisfied when processing personal data. These are:

1. **Consent**:
2. **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. **Legal obligation**: the processing is necessary to comply with the law.
4. **Vital interests**: the processing is necessary to protect someone's life.
5**. Public task**: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
6. **Legitimate interests**: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Special Categories of Personal Data

The following list is a list of personal data listed in the GDPR as a 'special category':

- 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

In order to lawfully process special category data, BHPS will identify both a lawful basis and a separate condition for processing. We will decide and document this before we start processing the data.

Use of Biometric Information
Bramcote Hills Primary School currently holds no biometric information. If biometric information is used in the future, the school will:

- obtain the written consent of a parent before we take and process a child's biometric data
- treat the data with appropriate care and comply with data protection principles as set out in the Data Protection Act
- provide alternative means for accessing services where a parent or pupil has refused consent.

Authorised Disclosures
The School will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the school's authorised officer may need to disclose data without explicit consent for that occasion. These circumstances are strictly limited to:

- pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations
- pupil data disclosed to authorised recipients in respect of their child's health, safety, welfare and protection
- pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school
- staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters
- unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances, visitors and volunteers are required to sign a form agreeing not to disclose the data outside the school.

Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and teaching assistants will only be made available where the person requesting the information is a professional legitimately working within the school who needs to know the information in order to do their work. The school will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything that suggests that they are, or have been, either the subject of or at risk of child abuse.

Secure Storage of and Access to Data
The school ensures that systems are set up to minimise access by unauthorised users and data breaches.
Members of staff are not, as a matter of course, granted access to the whole management information system (Scholar Pack).
The School advises that all users use strong passwords made up from a combination of letters, numbers and symbols and that user passwords must never be shared.
Personal data is only accessed on machines that are securely protected. Any device that can be used to access personal data will be locked if left (even for very short periods) and set to auto lock if not used for ten minutes.
All storage media is stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
Personal data is only stored on school equipment.
Where possible, personal data is anonymised e.g. by the use of initials rather than full name.
When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data will be encrypted and password protected
- the device will be password protected
- the device will offer approved virus and malware checking software.

The school has a clear policy and procedure for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups and a disaster recovery plan.

Bramcote Hills Primary School ensures that data storage through online systems and data held in remote and cloud storage is still protected in line with the Data Protection Policy. The school will ensure that it is satisfied with controls put in place by remote /cloud based data services providers to protect the data. Cloud-based services will only been used for pupil work and education resources.
All paper based personal data is held in lockable storage.

Subject Access Requests
Data subjects have a number of rights in connection with their personal data:

- Right to be informed – Privacy notices
- Right of access – Subject Access Request
- Right to rectification – correcting errors
- Right to erasure – deletion of data when there is no compelling reason to keep it
- Right to restrict processing – blocking or suppression of processing
- Right to object – objection based on grounds pertaining to their situation
- Right to object to direct marketing
- Right to be notified of any changes in relation to these rights
- Rights related to automated decision making, including profiling.

At Bramcote Hills Primary School, procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know:

- if the data controller holds personal data about them
- a description of that data
- the purpose for which the data is processed
- the sources of that data
- to whom the data may be disclosed

The data subject has the right to a copy of all the personal data that is held about them. The school provides the information free of charge, however a 'reasonable fee' may be charged where the request is manifestly unfounded or excessive, especially if this is a repeated request.

Secure Transfer of Data and Access Out of School
The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- when restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should have secure remote access to the management information system
- if secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) help organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. Where the use of personal data involves any of the following, Bramcote Hills Primary School will complete a DPIA:

- the processing of large volumes of sensitive data
- large-scale monitoring of the public
- automated decision making / profiling
- when new technologies are adopted that involve processing of personal data
- when using profiling or special category data to decide on access to services
- when processing biometric or genetic data
- when collecting personal data from a source other than the individual without providing them with a privacy notice (invisible processing)
- if tracking individuals' location or behaviour
- if profiling children or targeting marketing or online services at them
- when processing data that might endanger the individual's physical health or safety in the event of a security breach.

The DPIA will contain:

- a description of the processing operations and the purpose
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that we comply.

Disposal of Data

Bramcote Hills Primary School has a Document Retention Schedule that defines the length of time data is held before secure destruction. The Information and Governance Framework for schools provides support for this process and Bramcote Hills Primary School has adopted this advice. The school ensures the safe destruction of paper personal data through shredding when it is no longer required or safe disposal of electronic equipment through registered safe disposal companies.

Audit Logging / Reporting / Incident Handling

In accordance with the GDPR Data Protection laws, Bramcote Hills Primary School will keep records of processing activity. This will include:

- the name and contact details of the data controller
- where applicable, the name and contact details of the joint controller and data protection officer
- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the data has been collected
- under what lawful basis processing is being carried out
- where necessary, how it is retained and destroyed
- a general description of the technical and organisational security measures.

Bramcote Hills Primary School endeavours to maintain good auditing processes. Audit logs will:

- provide evidence of the processing activity (Information asset register and Data Flow) and the DPIA
- record where, how and to whom data has been shared
- log the disposal and destruction of the data
- enable the school to target training at the most at-risk data
- record any breaches that impact on the data.

All data breaches are recorded. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, or could result in the affected person/people coming to significant harm, then the DPO will report the breach to the ICO. The record will ascertain:

- a ‘responsible person’ for each incident
- a communications plan, including escalation procedure
- a plan of action for rapid resolution
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents will be reported through the DPO to the Information Commissioner’s Office within 72 hours of the breach being detected.

Training & Awareness
All staff will receive data protection training as part of the school induction process and will be made aware of their responsibilities. This training will be refreshed annually.

Policy Review Date – September 2019

Linked Documents
Data Protection Officer Responsibility Profile
Senior Risk Information Officer Profile
Information Governance Board Terms of Reference
BHPS Privacy Notice