DATA PROTECTION POLICY

Spring 2019

Manager

Mrs J Hill

Review Date – Spring 2022

Aims & Objectives:

The aim of this policy is to provide a model set of guidelines to enable staff, parents and pupils to understand:

- The law regarding personal data
- How personal data should be processed, stored, archived and deleted/destroyed
- How staff, parents and pupils can access personal data

The objective of the policy is to ensure that the school acts within the requirements of the Data Protection Act (DPA) of 2018 and the General Data Protection Regulations (GDPR) when retaining and storing personal data, and when making it available to individuals.

What is the GDPR?

GDPR is a European Directive that was brought in UK law with an updated Data Protection Act for May 2018. Brexit will not change it.

The Data Protection Act 1998 has been repealed and replaced with the Data Protection Act 2018.

The GDPR and new DPA exist to look after an individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As Public Bodies, school have more obligations than some small businesses. It is mandatory to comply with the GDPR and proposed provisions in the new Act. We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is 'data'?

Any information that relates to a living person that identifies them. This can be by name, address or phone number, for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data and biometric data where processed to uniquely identify a person. Schools often collect sensitive data for Department for Education and Local Authority requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Every school also has to publish a Privacy Notice on the website.

What are the key principles of GDPR?

School must have a legitimate reason to hold the data: we explain this in the Privacy Notices on the school website. We often ask for consent to use data about a pupil for a particular purpose. If

you wish to withdraw consent, we have a form to complete to allow us to process your request (see Withdrawal of Consent section of this policy). There is some data that you cannot withdraw your consent from us keeping, as explained in the 'Data Subject Rights' section of this policy. Data cannot be use for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited Collection
Data Controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack, only limited information can be lost.

Accuracy
Data collected should be accurate, and steps should be taken to check and confirm accuracy. We do this when pupils join the school and check on an annual basis.
If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms.

Retention
We have a Data Retention Policy that explains how long we store records for. This is available on request or in the GDPR section of the school website.

Security
We have processes in place to keep data safe. That might be paper files, electronic records or other information. We retain hard copies of personal data and sensitive personal data in files in locked cupboards and electronic data is stored on password protected computers or on the school server which can only be accessed by staff with verified staff accounts. The back up on the school server is also password protected. Laptops containing such data are encrypted to provide extra security. Staff have been trained on the requirements of GDPR and take care to ensure that they only store data that they need in order to perform their duties. Laptops are not left unattended in vehicles when staff take them to work off site. Emails containing personal data are sent securely to outside agencies using the Egress system and staff send emails regarding pupil data using their secure school Outlook accounts.

Who is a 'Data Subject'?
Someone whose details we keep on file. Some details are more sensitive than others. For example, the GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data Subjects' Rights
Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected.

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data Subjects' rights are also subject to child protection and safeguarding concerns, and sharing information for the prevention and detection of crime. Schools also have a legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC, amongst others. In some cases, these obligations override individual rights.

Subject Access Requests
You can ask for copies of information that we hold about you or a pupil who you have parental responsibility for or are a parent of at school. The Subject Access Request process is set out separately (see Appendix 1). You need to fill out the form (see Appendix 2), and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if, for example, the school was closed for holidays. The maximum extension is up to two months.

When we receive a request we may ask you to be more specific about the information that you require: this is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information in an electronic form.

If you wish to complain about the process, please see our Complaints Policy and later information in this policy.

Who is a 'Data Controller'?
Our school governing board is the Data Controller. They have ultimate responsibility for how school manages data. They delegate this to data processors to act on their behalf.

Who is a 'Data Processor'?
This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the LA.

Data Controllers must make sure that data processors are as careful about the data as the controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing Data
School must have a reason to process the data about an individual. Our privacy notices set out how we use data. The GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach, we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the Data Controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

Data Sharing

Data sharing is done within the limits set by the GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

Breaches & Non-Compliance

If there is non-compliance with the policy or processes, or there is a DPA breach as described within the GDPR and DPA 2018 then the guidance set out in the Breach & Non-Compliance Procedure needs to be followed (see Appendix 3).

Protecting data and maintaining Data Subjects' rights is the purpose of this policy and associated procedures.

Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the GDPR as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*

Consent and Renewal

On the school website we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

Parental Consent Procedure

On arrival at school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the data collection/consent form which will be available on our school website for the next academic year.

We review the contact and consent form on an annual basis. Forms will be sent out for parents to return to school in order to keep parental consent up to date.

Pupil Consent Procedure

Where processing relates to a child under 16 years old, school will obtain the consent from a person who has parental responsibility for the child.

Because all our pupils are aged below 13, they will not usually be asked to give consent or be consulted about how their data is obtained, shared and used.

Staff Consent Procedure

Staff may be asked to consent to the storing and sharing of information that is above and beyond what is set out contractually or in the Staff Handbook. This will be done when necessary and staff will be given clear guidance on how long the data will be retained and how it will be destroyed.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles. Forms are on our website or available on request from the school office.

Data Protection Officer
We have a Data Protection Officer whose role is to:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the GDPR
- to monitor compliance with the GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- To be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the GDPR

Our DPO is John Walker whose contact details are:
Company – Flint Bishop Solicitors
Address – Office 7, The Courtyard, Gaulby Lane, Stoughton, Leicestershire, LE2 2FL
E-mail – john.walker@flintbishop.co.uk

Physical Security
In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.
The School Business Manager is responsible for authorising access to secure areas along with the other members of the Senior Leadership Team.
All staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

Secure Disposal
When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.
These processes, when undertaken by a third party are subject to contractual conditions to ensure GDRP and DPA compliance.

- Hardware is disposed of/recycled by Mr Jonathan Butler (Media Technician)
- Hard copy files are destroyed by any member of staff who hold them, but in particular by the office staff.
- Servers and hard drives are cleansed by L.E.A.D. I.T.
- Portable and removable storage is destroyed/cleaned/recycled by Mr Jonathan Butler.

Complaints & the Information Commissioner Office (ICO)
The school Complaint Policy deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

Appendix 1

Subject Access Request (SAR) – Process

As an organization, we collect and process data about individuals. We explain what information we collect, and why in our Privacy Notices.

Any individual, or person with parental responsibility, or young person with sufficient capacity to make a request is entitled to ask what information is held. Copies of the information shall also be made available on request. A form to complete is available. Please download the form from the GDPR section of the school website or ask for a paper copy in the school office.

To ensure that requests are dealt with in an effective and timely manner we may seek to clarify the terms of a request.

To collate and manage requests we have designated Mrs Jules Hardisty, our School Business Manager to co-ordinate all requests.

Evidence of their identity, on the basis of the information set out and the signature on the identity must be cross-checked to that on the application form. Discretion about employees and persons known to the school may be applicable but if ID evidence is not required an explanation must be provided by school staff and signed and dated accordingly.

Exemptions to a SAR exist and may include:

- Education, Health, Social Work records
- Examination marks and scripts
- Safeguarding records
- Special educational needs
- Parental records and reports
- Legal advice and proceedings
- Adoption and Court records and/or reports
- Regulatory activity and official requests e.g. DfE statistical information
- National security, Crime and taxation
- Journalism, literature and art
- Research history, and statistics
- Confidential references

All data subjects have the right to:

- know what information is held
- know who holds this information
- know why this information is held
- know what the retention period is for this information
- know that each data subject has rights. Consent can be withdrawn at any time (to some things).
- request rectification, erasure or to limit or stop processing
- complain

Many of these questions will be answered within the Privacy Notices or the Retention Policy on the website.

The information will be provided in an electronic format, usually within one calendar month of the request. However in some circumstances, for example the school is closed for holidays, this may be extended by up to another calendar month.

Appendix 2

Subject Access Request Form

Data Subject (person who information is about)

Title	
Name	
Date of Birth	
Year group (if child or young person)	

Person Making the Request

Name	
Date of Birth	
Address	
Email Address	
Contact Phone Number	
Identification Evidence Provided (if required) Passport Driving licence or two from: Utility bill within last 3 months Bank statement of last three months Council Tax bill Rent book	

Status of Person Making Request

Parent or person with Parental Responsibility	
Are you acting on their written authority (please provide a copy of the consent)?	
If not the parent or with PR, what is your role?	

Details of Data Requested

Declaration

I, ……., hereby request that Gayton Junior School provide the data requested about me.

Signature: Date:

I, ……., hereby request that Gayton Junior School provide the data requested about ……..(insert child's name) on the basis of the authority that I have provided.

Signature: Date:

All staff (including visitors, volunteers and contractors) and governors must be aware of what to do in the event of a Data Protection Act/GDPR breach. The Data Breach Management Flowchart (see Appendix 1) outlines the process.

The Data Breach Form must be completed and updated as the process progresses.

Most breaches, aside from cyber-criminal attacks, occur as a result of human error. They are not malicious in origin and, if quickly reported, are often manageable.

Everyone needs to understand that if a breach occurs, it must be swiftly reported. Examples of breaches are:

- Information being posted to an incorrect address with results in an unintended recipient reading that information.
- Loss of mobile or portable data devices, such as an unencrypted mobile phone, USB memory stick or similar.
- Sending an email with personal data to the wrong person.
- Dropping or leaving documents containing personal data in a public place.
- Personal data being left unattended at a printer, enabling unauthorised persons to read that information.
- Not securing documents containing personal data (at home or work) when left unattended.
- Anything that enables an unauthorised individual access to school buildings or computer systems.
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role, e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What to do?

Being open and honest about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the Information Commissioner's Office (ICO) and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach as soon as possible to the Data Protection Compliance Manager (Headteacher) and Data Protection Officer (DPO) as soon as possible: **this is essential.**

The breach notification form will be completed and the breach register updated.

If the personal data breach is likely to risk the rights and the freedoms of the data subjects affected by the personal data breach, notification to those people will be done in a co-ordinated manner with support from the DPO.

The breach report must be made within 72 hours of becoming aware of the breach. It may not be possible to investigate the breach fully within the 72-hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO. The Chair of Governors will also be informed at this stage.

Investigation

In most cases, the next stage is for the Data Protection Compliance Manager or the DPO to fully investigate the breach. The Data Protection Compliance Manager or the DPO should ascertain whose data was involved in the breach, the potential effect on the Data Subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data
- Its sensitivity
- What protection was in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff members, suppliers, etc.) and whether there are wider consequences to the breach.

A clear record should be made of the breach in the school's log.

Procedure – Breach Notification: Data Controller (School) to Data Subject

For every breach, the school will consider notification to the Data Subject or subjects as part of the process. If the breach is likely to be high risk, they will be notified as soon as possible and kept informed of actions and outcomes.

The breach process will be described in clear and plain language.

If the breach affects a high volume of Data Subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the Data Compliance Manager and the Data Protection Officer.

Advice will be taken from the ICO about how to manage communication with Data Subjects if appropriate.

A post-breach action plan will be put into place and reviewed.

The Data Protection Compliance Manager, with support from the DPO if necessary, will review both the causes of the breach and the effectiveness of the response to it. This should be reported to the governing board for further discussion. Action plans should be made to address any identified systematic problems or if risk assessments indicate possible recurrence of the breach. If the breach warrants a disciplinary investigation, the Data Protection Compliance Manager will liaise with HR support for advice and guidance.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an

internal process (which can include disciplinary proceedings), it may be a source of information for the ICO or it could also be used within criminal or civil proceedings.

This process will be conducted by the Data Protection Compliance Manager or the DPO; this will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of the evidence that has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

Date	Evidence Description	Secure storage location & confirmed date	School Officer

Appendix 1

Data Breach Management Flowchart