



Friesland School – GDPR Policy (May 2018)

General Statement

The Head teacher and Governors of this School intend to comply fully with the requirements and principles of the General Data Protection Regulations (GDPR), which comes into force on the 25th May 2018. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities within these guidelines.

What is the GDPR?

This is a European Directive that will be brought into UK law with an updated Data Protection Act from 25th May 2018. Brexit will not change it.

The current Data Protection Act 1998 will be repealed and replaced with the Data Protection Act 2018.

What is the point of the GDPR?

The GDPR and new DPA exist to look after 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.

GDPR applies to everyone including schools

As Public Bodies schools 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 DfE and LA 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.

Friesland School has updated its Privacy Notices and are available on our website, or on request.

What are the key principles of GDPR?

The key principles are lawfulness, transparency and fairness.

We must have a legitimate reason to hold the data, we explain this in the Data Privacy Notices on the 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. There are sometimes when you cannot withdraw consent as explained in 'Data Subjects Rights'.

We will collect data for a specific purpose and use it only for that purpose

So, data cannot be used 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 will check this 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

Friesland school retains data records and follows guidance in line with legislation and common practice. The guidance explains how long we store records for. This is available on request.

Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information. Electronic sensitive data is stored safely and is password protected. Hard copy sensitive data is kept securely locked away. These processes will be reviewed and updated as relevant within 6 months of this policy.

Who is a 'data subject'?

Someone whose details we keep on file. Some details are more sensitive than others. 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 subject rights are also subject to child protection and safeguarding concerns, sharing

information for the prevention and detection of crime. Schools also have 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

Parents/Carers can ask for copies of information that we hold about them or a pupil who they have parental responsibility for or are a parent of at school. This Subject Access Request process is set out separately. Parents/Carers need to fill out the relevant form, and 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 the requester to be more specific about the information required. This is to refine any queries to make sure the parent accesses what is needed, rather than sometimes getting a lot of information that may not be relevant to the 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 parents 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, or contact the school for guidance.

Who is a 'data controller'?

Friesland school and its governing body 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 local authority.

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

The 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 and Process needs to be followed.

Protecting data and maintaining data subject's rights is the purpose of this policy and associated procedures.

The Breach & Non Compliance Procedures are attached as Appendix 1

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".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

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.

For Pupils and Parents/Carers

On admission to the 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.

We review the contact and consent form on an annual basis. It is important to inform school if details or your decision about consent changes. A form is available.

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.

Pupil's may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

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.

Please complete the appropriate form.

CCTV Policy

Please also see the CCTV Policy

We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:-

Detection and prevention of crime

School staff disciplinary procedures

Pupil behavior and exclusion management processes

To assist the school in complying with legal and regulatory obligations

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 J A Walker, Solicitor, whose contact details can be supplied on request.

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 Site Manager is responsible for authorising access to secure areas along with the Head, Leadership Team, Business Manager and Health and Safety Officer.

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 GDPR and DPA compliance.

Hardware is disposed of by engaging with a bona fide organisation after careful examination of their policies and processes for doing so. This is to ensure all information that may exist is removed or destroyed in a compliant and confidential manner.

Physical records containing confidential data are disposed of and shredded by Smurfit Kappa Security Shredding.

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.

You can complain if you have asked to us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

Review

A review of the effectiveness of GDPR compliance and processes will be conducted by the Data Protection Officer every 12/24 months.

Appendix 1

Data Protection Breach & Non Compliance Procedure

All staff, governors and trustees must be aware of what to do in the event of a DPA / GDPR breach.

The 'Data Breach Flowchart' 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 which results in an unintended recipient reading that information
- Loss of mobile or portable data device, 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.
- 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 equipment (and subsequently its records), is 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 about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the 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 to the Data Controller, Data Protection Compliance Manager and 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 result in a risk to the rights and 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.

Signed by the Headteacher _____ Dated _____

Signed by Chair of Governors _____ Dated _____

Date Approved by Governing Body _____ Minute Number _____