PERRYFIELDS HIGH SCHOOL

"Together We Achieve Excellence"

Data Protection and GDPR Policy

Title: Data Protection & GDPR Policy			
Publication Date:	December 2019	Authorised by:	Governors
Revision:	2.0	Date Authorised:	December 2019
Last Review:	December 2019	Review Due:	December 2020

SIPS Education
Smarter Specialist Support

Health, Safety
& Facilities

Introduction – what is GDPR?

The General Data Protection Regulation replaces the Data Protection Act 1998, as of 25th May 2018. This regulation identifies certain principles that the school as an organisation that stores or processes 'Personally Identifiable Information' must be able to demonstrate compliance with. This policy along with the accompanying guidance has been put into place to ensure all staff and Governors in the school have an understanding of the scope of the regulation, how it affects them, and the working practices that must be employed on a day to day basis in order to safeguard the personal information of individuals, which we have and use within the school.

Applicability

This policy will apply to any member of staff in the school who processes **personally identifiable information**. Such individuals must ensure that they are familiar with the contents and behaviours identified within this policy, and should ensure they refer to this policy and guidance when carrying out their duties.

Definitions and Common Terminology:

- Data Subject: an identified or identifiable natural person (living)
- Personally Identifiable Information: any information relating to an identified or identifiable natural person
- Data Controller: a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
- Data Processor: a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller.
- Data Protection Officer: a person who is tasked with helping to protect PII, and helping an organisation to meet the GDPR compliance requirements. Does not hold ultimate accountability for compliance.
- Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data

ICO: Information Commissioners Office (Supervising Authority in the UK)

Principles

In accordance with the obligations placed upon the school as a Data Controller, personal data will be processed in accordance with the Principles of GDPR.

Legality, Transparency and Fairness

- Personal data will only be processed by the school, where it is able to demonstrate that it has a 'Lawful basis' for the processing activity.
- In order to do this, the school will undertake a data audit to identify and document those data sets / records held within the school, which contain personal information and in each case, document the lawful basis for processing.
- Without a lawful basis, processing must not take place, and the personal data should not be held by the school.

- The school will endeavour to ensure all Data Subjects are clear about the ways in which the school is processing its personal data.
- The Privacy Notice will be made readily available by posting this on the school website and making paper based copies available from the school office. A copy of the privacy notice will also be included in the schools' admissions packs.

Purpose Limitation

- Personal data will be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Internal records are maintained to reflect the purposes for which processing will take place.

Appropriate technical and organisational measures will be maintained in order to safeguard personal data and are further documented within the Privacy Impact Assessments.

Minimisation

- The personal data will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed.
- The school will periodically review its' data capture forms and processes, to ensure that the information being requested is not excessive, and that the school is not capturing more personal information than is required.
- Personal data collected by members of staff should, wherever possible, be limited to the scope of what is laid out in official school data capture forms.
- Wherever there is any uncertainty a referral should be made to the Data Protection Officer for further guidance.

Accuracy

- The school will take every reasonable step to ensure that personal data that is inaccurate is erased or rectified without delay.
- The school will take proactive steps to check the accuracy of information held within its systems and to subsequently carry out updates as required, through a variety of measures.

Storage Limitation

- Personal data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is being processed.
- Retention periods for the various records held in the school containing personal data, will be identified and documented.
- The school has decided to use the Information Records Management Society Toolkit as its' guide when determining the appropriate retention periods for documents. A copy of this toolkit is available to staff on the school server T: Drive GDPR folder or via www.irms.org.uk

- Archived, paper based documents are stored securely in locked filing cabinets and shredded at the end of their lifespan.
- Archived electronic records are held securely on the school server and backups are deleted once they reach the end of their lifespan.
- Folders are labelled to indicate when they need to be deleted and a search done once per month by the ICT Manager to highlight files that need to be considered for deletion.

Integrity and Confidentiality

- Personal data is processed in a manner which ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical and organisational measures.
- Clear desk and clear screen - PCs **will not be** left unlocked when workstations are left unattended.
- Any paper based documents containing personal information will be secured at the end of the day, and when rooms / offices are left unattended.
- Positioning of computer screens will be considered carefully to ensure only authorised personnel are able to view sensitive or confidential information.
- Passwords for accessing systems must be complex enough to make it extremely difficult for third parties to break them.

Accessing and sharing information

There are many different ways in which School staff can access data. It is their responsibility to know if they are simply accessing the data that is stored securely elsewhere, or downloading or saving data to a School device.

It is important that employees understand the difference between accessing data (looking at or reviewing) via a mobile or off-site device and downloading/Saving data (this will save a copy of the information onto the mobile device you are using) to a mobile or off-site device. Data should not be downloaded or saved to a mobile or offsite device unless you can justify this action with a clear business case for doing so. Once the data is no longer required on the device it must be deleted immediately.

There are also times when it will be necessary to share information with others.

Inside the school:

- When sharing information with others within the school, if information is of a confidential, sensitive or personal nature, it must be treated as such. Information should only be shared with the individuals who require it, do not copy people into emails if they do not require access to the information contained within.

Outside the School:

- Secure transmission: Where possible, use recognised secure transmission methods such as Move-it and Secure Access via DFE Sign In.

- Never send personal data within a normal email. If email is the only method of transmission available, ensure the information is included in a password protected document.
- The password must be agreed with the email recipient in advance and not via the same email address.
- Ensure that the request for data is a valid one and that only the required data is provided. Always check why people require the data they ask for.
- Make sure that the data is up to date. Check the accuracy of the data to be sent before sending.
- School Emails should never be sent to public email addresses.

When sending information (including letters) via post the following must be adhered to:

- Always get a second person to check the address is correct before sending.
- Pay particular attention to numbers as these are easily transposed, however, be aware the responsibility for the accuracy is still with the sender not the checker.
- Always use window envelopes if the address is pre-populated on the enclosed letter to avoid transcription errors or typed labels to avoid issues in relation to legibility of handwriting.
- Always ensure that envelopes are securely sealed. Use additional methods such as sticky tape, glue or staples if deemed necessary.
- Double check that no additional information has been included that is not relevant e.g. something mistakenly attached.
- If a request is received from an outside agency such as the Police, this should be referred in the first instance to the Data Protection Lead and DSL.

Storage of Data on Portable/External Devices

- The loss of any device that can send, store or retrieve data must be reported to your Data Protection Lead and the Data Protection Officer immediately.
- Devices that are capable of transmitting and receiving data information, such as smartphones, should only be used for the purposes for which they were supplied and must be protected by a strong secure password.
- Anyone who uses portable devices to access or store data is responsible for the information which is transported within. This includes USB flash memory devices (“memory sticks”), laptops, external hard disk drives, mobile phones, tablets. Be aware of devices that can access information, such as emails, that could contain sensitive data.
- Any memory stick/portable device that you use for the transport or storage of personal or sensitive nature must be encrypted to an appropriate standard and approved for use by our Data Protection Lead / IT Support.
- All portable devices must be encrypted, and care must be taken to safeguard the equipment against loss or damage.
- Any storage devices no longer required which may contain information that is surplus to requirements or any device that is in need of secure disposal should be returned to our IT staff or the Data Protection Lead, in person.

- Media such as CDs or DVDs which contain data and are no longer required must be physically destroyed.

Paper and Manual Filing Systems

- Paper based (or any non-electronic) information must be assigned an owner.
- A risk assessment should identify the appropriate level of protection for the information being stored.
- Paper and files in the school must be protected and stored securely.

Security of Equipment and Documents Off-Premises

- Information storage equipment, data, software or any documents containing personal, sensitive or confidential data should not be used off-site without authorisation from the Head Teacher.
- Security guidelines must be adhered to for all equipment and documents taken offsite.
- Data must be protected against the possibility that it could be stolen, lost or otherwise divulged by physical (or non-electronic) means.
- Our premises are protected by door locks and access codes. It is important that the codes remain secure as these form part of our physical security procedures and as such help to keep our personal, sensitive and confidential data safe.
- Doors and windows must be locked when unattended and external doors (including loading bay/fire doors) must be locked when not in use.
- All visitors must sign in and receive a Visitor's Authentication Badge.
- All Visitors/Attendees should be supervised at all times and are required to wear visible authorised identification, and to record their date/time of entry/departure and person(s) being visited.

Accountability

The data controller will be able to demonstrate compliance with the previous principles. The school will do this by employing measures including:

- Ensuring a Data Protection Officer (DPO) is appointed (For our school the Data Protection Officer is provided to us by SIPS Education, and is contactable via gdpr@sipseducation or 0121 296 3000).
- On a day to day basis, the first point of contact within the school is the data Protection lead (Mr S Gibson); the Data Protection lead will liaise with the Data Protection Officer for advice and guidance as required.
- The DPO will undertake periodic monitoring activities to help ensure compliance with the regulation. They must be informed of any suspected data breach, and will help to investigate circumstances surrounding breaches, and ascertain whether they are required to be reported to the ICO.
- The DPO must also be informed of any Subject Access Requests that are submitted to the school, and will assist in making the response to the Data Subject.

- The Governing Body will be kept informed of our ongoing compliance via reports, which will include an overview of any data breaches that have occurred along with actions taken, and any Subject Access Requests received and responded to.
- Training for staff and Governors will be provided by the DPO on an annual basis, and further supplemented by reminders in school on policy and procedures to follow to safeguard personal data.
- Where the school needs to share personal data with 3rd party organisations (Data Processors), it will ensure that adequate steps have been taken to vet the robustness of the Processors systems in order to safeguard the information shared, and will maintain a written record of this.
- Data Protection will be considered as part of all project planning, when we are reviewing our systems for data collection and data processing. Where required, we will undertake Data Protection Impact Assessments to ensure appropriate measures are put in place to safeguard the data, to prevent breaches and ensure compliance with the requirements of the regulation.

The rights of the Data Subject

Under the Regulation, Data Subjects have 8 rights, as listed below. The School will ensure procedures are in place to be able to respond in a timely manner to any request from a Data Subject to exercise one of their rights. The Data Protection Lead in the school will liaise with the DPO as required, to ensure an appropriate response.

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Subject Access Requests

- If a data subject wishes to see copies of the information held on them by the School, they may submit a Subject Access Request.
- Such requests must be made in writing in order to be valid.
- Any such requests received by members of staff must immediately be forwarded to the Data Protection Lead who will liaise with the DPO in order to make the response.
- No member of staff may divulge personal information over the phone, or respond to such a request without the express consent of the Data Protection Lead.
- Responses to SARs must normally be made within one month.
- A further 2 months may be used in exceptional circumstances only, and only with the agreement of the DPO.

Procedures for Responding to Data Breaches

- If any member of staff becomes aware of a data breach situation, they must ensure this is reported to the Data Protection Lead as soon as possible
- The school is obliged to keep a record of all breaches and investigate them to an appropriate level.
- Some breaches of a more serious nature will need to be reported to the ICO.
- The DPO will help the school to ascertain whether a breach is reportable, and will advise on all such occasions if this is the case.
- The Data Protection Lead will liaise with the DPO to determine whether a breach is reportable or not.
- Any near misses must be reported so that we can learn from these also, and use them as a way of informing future revisions to our policies and/or procedures for data protection.

Changes to this policy

We reserve the right to change this policy at any time. Where appropriate, we will notify individuals of these changes by mail or email.