Data Protection Policy

Bleakhouse Primary School

Version 2.0

September 2020

1. 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 any organisation who stores or processes 'Personally Identifiable Information' must be able to demonstrate compliance with. This policy has been out 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.

2. Applicability

This policy will apply to any member of staff in the school who process 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 when carrying out their duties.

3. 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)*

4. 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. The following section lays down how this will happen in practice on a day to day basis.

4.1 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 data audit will be held on **the Staff Shared Area of the Network (GDPR Folder)** and should be considered to be a 'live' document. All staff may be asked periodically to assist in reviewing the data audit to ensure all data sets currently in use within the school have been captured and considered, and a lawful basis for processing identified in each occasion.

The school will endeavour to ensure all Data Subjects are clear about the ways in which the school is processing its personal data. This will include publishing information on the type of personal data being collected, the lawful basis for processing, and types of other organisations who the information is shared with, within a privacy notice.

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.

4.2 Purpose Limitation: *personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.*

Internal records will be maintained to reflect the purposes for which processing will take place. More specifically, this will be included on the data audit record, and will include a record of the purpose, description of the categories of individuals and personal data, the categories of recipients of the data (e.g. 3rd party organisations who the School shares the data with); retention schedules for the personal data.

Appropriate technical and organisational measures that must be maintained in order to safeguard personal data are identified in this policy in general, and will be further documented within Privacy Impact Assessments, if the processing of personal data is higher risk and could result in a risk to the rights and freedoms of the individual.

4.3 Minimisation: *the personal data must be 'Adequate, relevant and limited to what is necessary in relation to the purposes for which they are 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 about the level of information being requested from Data Subjects, a referral should be made to the Data Protection Officer for further guidance.

4.4 Accuracy: *every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*

The school shall 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. These include, but are not limited to:

- Issuing data capture forms on an annual basis to parents/Guardians to verify the accuracy of personal information held on the SIMS system, including: emergency contact details; correspondence address; medical details of the pupils etc.
- Checking attainment data in systems on a regular basis, through the use of pupil progress meetings;
- Checking accuracy of staff details via annual data collection sheets to staff for data checking and amending where necessary

4.5 Storage Limitation: *Personal data shall 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 are processed*

Retention periods for the various records held in the school containing personal data, will be identified and documented as part of the data audit activity.

The school has decided to use the Information Records Management Society Toolkit as it's' guide when determining the appropriate retention periods for documents. A copy of this toolkit is available to staff within the Staff Shared Area of the Network (GDPR Folder) or via www.irms.org.uk

All documents at the end of their lifespan are shredded by a confidential waste shredding company – on site.

This is achieved by the contract held with Restore Data Shred.

IT Equipment is securely destroyed with Recycle IT for U Ltd – all equipment destroyed is listed with Serial Numbers and information given to the school.

4.6 Integrity and Confidentiality: *Personal data will be 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 or organisational measures*

Clear desk and clear screen:

PCs should not be left unlocked when workstations are left unattended. PCs can be locked by *e.g. hitting the windows and L keys – this will vary dependant on your operating systems.*

Any paper based documents containing personal information should be secured at the end of the day, and when rooms / offices are left unattended. Where there are any concerns over the availability of secure (lockable) storage, or clarification required over the type of information that needs to be secured, staff should in the first instance speak with *Head Teacher/Deputy Head Teacher or Business Manager* who will liaise with the Data Protection Officer if required.

Positioning of computer screens should be considered carefully to ensure only authorised personnel are able to view sensitive or confidential information. This is of particular importance within areas accessed by members of the public, such as the reception area. Privacy screens will be considered where positioning of screens alone will not address this concern.

Passwords and protection of hardware:

Passwords for accessing systems must be complex enough to make it extremely difficult for third parties to break them: passwords should be at least 8 characters long, have a mixture of upper case and lower case letters, at least one number and one character.

Passwords should be changed every 42 days in line with the Sips IT Policy and never shared with any other member of staff / shared amongst other users.

Each computer has a lock out period for inactivity that is set by the system manager, these can be set from 5 minutes to 45 minutes depending on the user (DSL / HT / Office usually 5 minutes / class computers can be set for longer periods).

Password Policy has been reviewed and updated – SIPs IT October 2020 (See GDPR Evidence Folder)

Mobile devices (including phones, tablets and laptops) must be protected to the same high standard.

You must:

- Activate the built in security PIN and set this to the most secure level (if the device allows, this should always be a secure password as detailed above or fingerprint recognition rather than a 4 digit pin;
- Ensure that you have a copy of IMEI numbers for the phone and the SIMS stored securely to allow deactivation in the event of loss.

You are personally responsible for any information accessed or disclosed on these devices so it is imperative that you keep your password safe and secure, and do not share it with anyone else.

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. Office 365 and the tools it provides allows employees to not only access their emails but actually open, modify, save and /or send any data that is held.

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.

The following security measures have been put in to place:

- ***Staff Laptops have 'Bitlocker' security installed – on power-up staff are required to enter a security code – without the code the device is rendered useless***
- ***Staff have been given VPN access – allowing working from home to save to the Network rather than the device being used, therefore no sensitive data is stored on to laptops***
- ***There is a built in warning on Sophos that will warn users when they are trying to copy documents / images onto a memory stick, it will block anything that it deems to be Pll as Sophos is clever enough to read the files and work out what is sensitive and what is not.***

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. Delete sensitive, confidential or personal information once it has been used for the purpose it has been collected and is no longer required.

Outside the School:

Where more than one piece of personal, sensitive or confidential data is to be sent, one of several methods can be used. If in doubt please check with the Data Protection Officer.

- Secure transmission: Where possible, use recognised secure transmission methods such as WebEx.
- 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 via telephone, not in another email. Never include the password in the email to which the password protected document is attached, nor send the password via another email (if the first email is intercepted, then the second could also be).
- 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 – if in doubt check with the Data Protection Lead before sending.
- 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 (e.g. Hotmail, Gmail etc.) regardless of what they contain, unless this has been clearly identified by the recipient as their business email address.

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. Only send relevant data. Check that it is valid and accurate and no additional information i.e. additional sheets are included in error.
- 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

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. The password used to encrypt information must not be written down and must never be stored or transported with the device. Please be aware an encrypted memory stick/portable device will ALWAYS ask you for a password before use.
- 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. If you do not have the means to do this, please pass them to the IT Department/Data Protection Lead for disposal – stating clearly that they contain sensitive information
- All portable devices must be encrypted, and care must be taken to safeguard the equipment against loss or damage. The password used to encrypt information must not be written down and must never be stored or transported with the device.

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 by one of the following measures:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes
- Stored in a Secure Area protected by access controls

It is important that someone has ownership i.e. takes responsibility for the storing and protecting of such systems.

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.

Information storage equipment includes items such as personal computers, organisers, tablets, mobile phones and external storage devices.

The following security guidelines must be adhered to for all equipment and documents taken offsite, it must:

- Not be left unattended in public places.
- not be left unattended in a vehicle unless the property is concealed from view and all doors are locked, windows and the roof closed and fastened, all security devices on the vehicle are put in full and effective operation and all keys/removable ignition devices removed from the vehicle
- not be left open to theft or damage whether in the office, during transit or at home
- where possible, be disguised (e.g. laptops should be carried in less formal bags)
- be returned to the School as soon as is practically possible.
- Where it is necessary to transport sensitive or personal data in this manner, data encryption must be in place, and manufacturer's instructions for protecting the equipment should be observed at all times

Physical Security

Our data must be protected against the possibility that it could be stolen, lost or otherwise divulged by physical (or non-electronic) means. This section is related to building security and the level of care that you are expected to provide when transporting computers or paper files outside of the building.

- 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. This is issued by the staff in Reception and applies to all Visitors.
- 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.
- Confidential data or computer systems that contain such data. If such access is requested, it is the employee's responsibility to ensure it is a legitimate request and data protection is not breached.
-
- If in doubt, please check with your Data Protection Lead or the Data Protection Officer.

Use of Fax

Please be aware that a Fax should be used as a communication method of last resort, where no other methods are available.

Outgoing Fax

DO NOT USE fax to transfer personal, confidential or sensitive information. Where fax is the only method of communication available:

- Use a cover sheet with a confidentiality statement.
- Contact the recipient to inform them a fax is being sent, and confirm that someone is at the fax machine waiting to receive it.
- Ask for confirmation upon receipt of the fax within an agreed time scale.

- Use programmed numbers wherever possible to avoid misdialling, or check the number before the fax is sent and dial carefully.
- On completion retain the printed record of transmission as confirmation the fax was successful. This may need to be requested if not automatic. Include it on file with a copy of the cover sheet as proof of sending.
- Documents should not be left unattended at the fax machine.
- If it is not possible to obtain confirmation upon receipt of the fax, the printed record of transmission (which may need to be requested if not automatic), should be kept on the appropriate file with the cover sheet, as confirmation that the fax was successfully transmitted.

Incoming Fax

There are risks associated with incoming fax. However, the main risk is with the originator of the fax as it is their responsibility to ensure that they are content with the arrangements

Any incoming faxes must be treated as a record and stored, archived and disposed of appropriately.

4.7 Accountability: *the 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 is appointed. This individual will have suitable knowledge and experience to fulfil this role and will have a direct line of report through to the Head Teacher and Governing body for data protection related matters.

On a day to day basis, the first point of contact within the school is the Data Protection lead (Office Manager); 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.

For our school the Data Protection Officer is provided to us by SIPS Education, and are contactable via gdpr@sipseducation.co.uk or 0121 296 3000.

Our Governing Body will be kept informed of our ongoing compliance via reports to Full Governors 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, prevent breaches and ensure compliance with the requirements of the Regulation. A copy of the Data Protection Impact Assessment is included at Appendix A.

5. 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

6. 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, so it is imperative that such requests are brought to the attention of the Data Protection lead without delay. 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, in order to ascertain what can be learnt from the circumstances surrounding each, and then used to review procedures as required with the aim of preventing a similar breach occurring again.

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.

Where breaches are reportable, the report must be submitted to the ICO within 72 hours of the school becoming aware of the breach, and so it is crucial the Data Protection Lead is notified of any potential breaches immediately.

You must also report any near misses 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.

Appendices:

Data Protection Impact Assessment Template