BETHANY SCHOOL DATA PROTECTION POLICY

Data Protection Act 2018

Incorporating the School Data Breach Procedure

March 2022

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. It also considers the provisions of the General Data Protection Act that became enforceable 25 May 2018 and has subsequently been updated to the UK GDPR, effective January 31, 2021.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-UK GDPR/principles/

Bethany School collects and uses personal information about staff, pupils, parents, and other individuals who come into contact with the school. This information is gathered to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

This policy statement applies to all School Governors, employees, other staff, and individuals about whom the School processes personal information, as well as other partners and companies with which the School undertakes it business. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Data Controllers

Schools are 'Data Controllers' under the Data Protection Act 2018 and must 'Notify' (register with), the Information Commissioner's Office on the following website, unless exempt: https://ico.org.uk/for-organisations/register/

We at Bethany School are the Data Controller for the purposes of the Data Protection Act. Bethany School is registered as such with the ICO (annually renewed)

Roles and responsibilities

Governing board – The governors have overall responsibility for ensuring that our school complies with all relevant data protection obligations

The Data Protection Compliance Manager (DPCM) – The DPCM for Bethany School is Mendes DeCastro. He is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law and developing related policies and guidelines where applicable. The DPCM will report their activities directly to the governing board, and where relevant, report to the board their advice and recommendations on school data protection issues. The DPCM can be contacted by email at: dataprotection@bethanyschoolsheffield.org

The Data protection Lead is the Head Teacher – He is responsible for liaising with the DPCM and acting in the first instance on data breach, representing the data controller on a day-to-day basis. He will also monitor the dataprotection@bethanyschoolsheffield.org email account to ensure that data requests are dealt with in a timely manner.

All staff Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPCM in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

Data Protection Principles

The GDPR is based on Data Protection Principles that our school must comply with. The principles say that personal information shall:

- be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions as set out in the 2018 Act are met;
- be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed;
- be accurate and, where necessary, kept up to date;
- not be kept for longer than is necessary for that purpose or those purposes;
- be processed in a manner that 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 ('integrity and confidentiality').

Procedures/Methods

- All staff (employed and voluntary) must take appropriate technical and organisational security measures to safeguard personal information.
- Personal information must be protected from unauthorised or accidental disclosure.
- Staff are responsible for ensuring that the personal information which they use during their role is appropriately secured and any concerns regarding its security are brought to the attention of The Head Teacher/DPCM This includes ensuring that personal information is removed from desks out of hours and sensitive personal information is locked in filing cabinets or desks when not in use.

- The Head Teacher/DPCM is responsible for ensuring that personal information when in use is only accessible by those with a need and right to access it to perform their function or role.
- Staff must respect the privacy of the subject of the personal information they are handling by treating personal information about others as we would expect information about ourselves to be treated.
- Careful consideration must be given to the transmitting of Personal Data. Personal data must not normally be transmitted **externally** via email. **Although it is acceptable to transmit personal data internally, you should consider choosing another method if possible.**
- Personal information must be disposed of safely and securely.
- Documents and any storage media containing input to and output from systems (paper or electronic) detailing personal information must be held, transported, and disposed of with due regard to its sensitivity.
- Where information is particularly sensitive it may be appropriate to ensure that the information is shredded on site.
- Publishing personal information on the Internet would make it available internationally therefore personal information must not be published on the internet, other than the names and work contact details of some employees and members if appropriate to their role.

Inappropriate and Unacceptable Use

Unacceptable use includes:

- unauthorised access of personal information
- unauthorised disclosure of personal information
- unauthorised use of personal information (e.g., not for reason given to access personal information)
- non-adherence to the school's information-sharing protocol
- unauthorised deletion

Employee or customer personal information must not be used for:

- any illegal purpose;
- any purpose which is inappropriate in the workplace by virtue of the fact that it may cause embarrassment or distress to another person or may bring the school into disrepute;
- any purpose which is not in accordance with the staff member's role or job description.

This is not an exhaustive list. Cases where staff do not comply with this Policy or legislation will be dealt with under the Disciplinary Procedure and, depending on the circumstances; non-compliance may be deemed an act of gross misconduct.

Staff are required to notify an appropriate person, if they become aware, or suspect that personal information is being misused or handled inappropriately.

Collecting Personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**

- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services) for pupils under 13.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's records management policy.

Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings

- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Subject access requests and other rights of individuals

Subject access requests.

See 'Appendix 2: Actioning a Subject Access Request for more details'

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPCM. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPCM.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of a request made during term time. If the request is made during a holiday period the time to process the request may be longer.
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPCM. If staff receive such a request, they must immediately forward it to the DPCM.

Parental requests to see the educational record

Parents can at any time during term ask to discuss their child's educational record with the child's teacher. The teacher will then agree a suitable time and run through the educational record. Parents are encouraged to discuss their child's progress with the teacher at least once per term.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Display work within school
- In written information such as newsletters or school publicity
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Safeguarding and online-safety policy for more information on our use of photographs and videos.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPCM, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPCM will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPCM and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data security and storage/disposal of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must take due caution to keep it secure
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software or password protection is used to protect all portable devices and removable media which may contain personal data, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Complaints

In the event that a complaint is received regarding Subject Access complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Monitoring arrangements

The Governors and the DPCM is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary and **every 2 years** and shared with the full governing board.

Links with other policies

This data protection policy is linked to our:

- Online safety Policy and Acceptable use Rules
- Safeguarding Policy and code of conduct
- Data retention/destruction policy

Approved by Governors on: 08/03/2022

Review Date: Feb 2024

Appendix 1: Personal data breach procedure

Important Note

This procedure has been produced based on current UK General Data Protection Regulations (UK GDPR) information. As further updates are released this procedure may be updated to reflect the changes.

Bethany School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Bethany School and all school staff, Governors, volunteers, and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Bethany School if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the Commissioner

1. In the case of a personal data breach, the Data Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The Data Controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Commissioner to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by several factors. Several examples are shown below:

- Loss or theft of pupil, staff, or governing body data and/ or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment Failure.
- Poor data destruction procedures.
- Human Error.
- Cyber-attack.
- Hacking.

Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the data protection Lead or, in their absence the Data Protection Compliance Manager. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Data Protection Lead must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Data Protection Lead must inform the Chair of Governors and DPCM as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Data Protection Lead and DPCM must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School’s legal support should be obtained.

5. The Data Protection Lead or nominated person must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the relevant County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately by The Data PPCM/Lead.

c. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately, and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the DPCM/Lead to fully investigate the breach. The DPCM/Lead 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 protections were 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 nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPCM/Lead should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case-by-case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the DPCM/Lead should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and **full** Governors meeting for discussion. If systemic or ongoing problems are

identified, then an action plan must be drawn up to put correct these. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The DPCM/Lead should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision, and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with the DPCM/Lead or the nominated person

Appendix 1: Personal data breach procedure

This procedure has been produced based on current UK General Data Protection Regulations (UK GDPR) information. As further updates are released this procedure may be updated to reflect the changes.

Bethany School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Bethany School and all school staff, Governors, volunteers, and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Bethany School if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the Commissioner

1. In the case of a personal data breach, the Data Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The Data Controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Commissioner to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by several factors. Several examples are shown below:

- Loss or theft of pupil, staff, or governing body data and/ or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment Failure.
- Poor data destruction procedures.
- Human Error.
- Cyber-attack.
- Hacking.

Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the data protection Lead or, in their absence the Data Protection Compliance Manager. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Data Protection Lead must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Data Protection Lead must inform the Chair of Governors and DPCM as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Data Protection Lead and DPCM must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School’s legal support should be obtained.

5. The Data Protection Lead or nominated person must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the relevant County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately by The Data PPCM/Lead .

c. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately, and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the DPCM/Lead to fully investigate the breach. The DPCM/Lead 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 protections were 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 nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPCM/Lead should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case-by-case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the DPCM/Lead should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and **full** Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put correct these. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The DPCM/Lead should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision, and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with the DPCM/Lead or the nominated person

Appendix 2: Actioning a Subject Access Request

1. Requests for information must be made in writing, which includes email, and be addressed to the Headteacher or DPCM**.** If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- birth/ marriage certificate
- P45/P60
- credit card or mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights. For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent. , most subject access requests from parents of pupils at this school will not be granted without the express permission of the pupil. Parents at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, bearing in mind guidance issued from time to time from the Information Commissioner's Office.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests for all or part of the pupil's educational record, once officially received, is 15 school days. If the subject access request does not relate to the educational record, we will respond within 40 days (not working or school days but calendar days, irrespective of school

holiday periods). However, the 40 days will not commence until after receipt of fees or clarification of information sought.

6. The Data Protection Act 2018 allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40-day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil, or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested or provided at face-to-face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.