STEP BY STEP SCHOOL

Data Protection Policy

STEP BY STEP SCHOOL

Contents

Document Control

Summary of Changes, Document Author, Owner, Reviewers and Approvers

Version:	Version Date	Nature of Change
V1.0	23/05/18	Document created
V1.1	17/10/18	Document updated after review with new Head teacher at school.
V1.2	22/05/20	Document updated as part of its review process. Formatting changed to UK English Clare Eastwood added as document approver and reviewer.
V2.0	08/09/20	GDPR policy and this policy merged into a single policy.

Document Change Approvers

Name	Title
Gayle Adam	Head Teacher
Clare Eastwood	School Business Manager
Mark Norris	Information Security Officer

Document / Change Reviewers

Name	Title
Gayle Adam	Head Teacher
Clare Eastwood	School Business Manager
Mark Norris	Information Security Officer
Gayle Adam	Compliance Officer

Document Review Plans

This document will be reviewed and updated, if necessary as defined below:

- As required to correct or enhance information content
- Following changes to an ISO 9001/Q91 quality system standards
- Following any organizational changes or restructuring
- Following a 2-yearly review

How to find the latest level of this document

The latest version of this document may be obtained from Gayle Adam or is housed on the school's server.

Document Distribution

This document is automatically distributed to all change approvers after an update and upon request.

Introduction

STEP BY STEP school needs to gather and use certain information about individuals.

These can include data on staff, pupils, parents [1], customers, suppliers, business contacts, and other people the school has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Step by Step school's data protection standards and to comply with the law.

Our school aims to ensure that all personal data [2] collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the provisions of the Data Protection Act 2018.

It will also provide details on actions to be taken should a data breach be suspected.

Note:

1. The term parents will be used in this document and refers to any legal guardian of a pupil or child.
2. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1. Data Policy - why this policy exists

This data protection policy ensures Step By Step school:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risk of data breach.
- This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.
- To comply with the data protection laws to meet the school's requirements as a Data Controller and Data Processor.

1.1 Data protection law

The General Data Protection Regulation that came into effect in May 2018 describes how organisations – including Step by Step school – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR, is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and no excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of the data subjects.
7. Be protected in appropriate ways.
8. Not be transferred outside of the European Economic Area (EAA) unless that country or territory also ensures an adequate level of protection.

1.2 Policy scope

This policy applies to:

- The Step by Step School main sites.
- Any satellite sites owned or managed by Step by Step school.
- All staff and volunteers of Step by Step School.
- All contractors, suppliers and other people working on behalf of Step by Step school.

It applies to all data that the school holds relating to identifiable individuals, even if that information technically falls outside of the GDPR (Data Protection Act 2018). This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Date of Birth
- National insurance number
- Telephone numbers
- Medical information
- plus any other personal data that identifies an individual

1.3 Data protection risks

This policy helps to protect Step by Step school from some very real data security risks, including:

- **Breaches of confidentially**. For instance, information being given out in appropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the school uses data relating to them.
- **Reputational damage**. For instance, the school could suffer if hackers successfully gained access to sensitive data.

1.4 Responsibilities

Everyone who works for or with Step by Step school has some responsibility for ensuring data is collected, stored and handled appropriately.

Each member of staff that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility. Note some of these roles may not exist or be carried out by 3rd party suppliers:

- The **Governing body** is ultimately responsible for ensuring that Step by Step school meets its legal obligations. ensuring that the school complies with all relevant data protection obligation.
- The **Information Security Officer,** is responsible for:
    - Keeping the governing body updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data the school holds on them (also called 'subject access requests').
    - Checking and approving and contracts or agreements with 3rd parties that may handle the school's sensitive data.
- The **IT Manager (or IT supplier),** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any 3rd party services the school is considering using to store or process data. For instance, cloud computing services.
- The **Data protection officer,** is responsible for:
    - The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
    - They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.
    - The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

- Full details of the DPO's responsibilities are set out in their job description.
- Our DPO is Gayle Adam (Head Teacher) and is contactable via the school on 01342811852

- **All 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 DPO 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 they have a lawful basis to use personal data in a way
  - If they need to rely on or capture consent, 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

1.5 General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, staff can request it from their line managers.
- Step by Step School will provide training to all staff to help them understand their responsibilities when handling personal data. Training will be provided to all staff on a regular basis.

- Staff should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used, and they should never be shared. Our ICT system requires all staff to change their passwords frequently.
- Personal data should not be disclosed to unauthorised people, either within the school or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If the data is no longer required and can be deleted in line with any legal or regulator guidelines, then it should be deleted and disposed of in a safe and secure manner.
- Staff should request help from their line manager or the Information Security Officer if they are unsure about aspect of data protection.

1.6 Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager or Information Security Officer.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- Staff should make sure paper and printouts are **not left where unauthorised people can see them,** like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically,** it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between members of staff.
- If data is **stored on removable media** (like a USB drives for example), these should be kept securely and locked away when not being used.

- Data should only be stored on **designated drives and servers and** should only be uploaded to an **approved cloud computing service.**
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the school's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones that has a requirement to be backed up.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

1.7 Data Use

Personal data is of no value to Step by Step unless the school can make use of it adhering to one of the 6 lawful bases defined under the data protection law. However. It is when personal data is accessed and used that it can be at greatest risk of loss, corruption or theft. By adhering to the principles below, the school is protected from abuses of data by a third party.

- When working with personal data, staff should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. It should never be sent by email, as this form of communication is not guaranteed to be secure.
- Data must be **encrypted before being transferred electronically.** The IT Help desk can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area.**
- Staff **should not save copies of personal data on their own computers.** Always access and update the central copy of the data.
- 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 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.

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education. This data includes, but is not restricted to:

- Contact details
- Results of internal assessment
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

Once our pupils reach the age of 13, we are legally required to pass on certain information to funding Local Authorities, which has responsibilities in relation to the education or training of 13-19-year-olds.

We are required, by law, to pass certain information about pupils to specified external bodies, such as the funding Local Authority and the Department for Education, so that they can meet their statutory obligations.

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required by law to pass certain information about staff to specified external bodies, such as the Department for Education, so that they can meet their statutory obligations. Any staff member wishing to see a copy of information about them that the school holds should contact the Head Teacher.

1.8 Data accuracy

The law requires Step by Step School to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort the school should put into ensuring accuracy.

It is the responsibility of all members of staff who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming parent's details during a parents evening.
- Step by Step school should investigate ways to make it **easy for data subjects to update the information** held about them.
- Data should be **updated as inaccuracies are discovered.** For instance, if a parent cannot be reached on their stored telephone number, it should be removed from the database and replaced with the correct number.
- 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 record retention schedule.

1.9 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 enough 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, if 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 respond to an emergency 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

1.10 Subject Access Requests

All individuals who are the subject of personal data held by Step by Step are entitled to:

- Ask **what information** the school holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the school is **meeting its data protection obligations.**

When an individual contacts the school requesting their information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller Compliance.officer@stepbystep.org.uk. The data controller can supply a standard request form, although individuals do not have to use this.

As per the new GDPR regulations individuals will not be charged per subject request. The data controller will aim to provide the relevant data within 14 days but depending on the amount of data it may take the full 30 days imposed under GDPR.

The data controller will always verify the identity of anyone making a subject access request before handing over any information by following the Subject Access Request Process.

The process for handling Subject Access Requests is defined in a separate document and should be followed when any request to supply data is received.

1.11 Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Step by Step school will disclose the requested data. However, the data controller will still ensure the request is legitimate, seeking assistance from the governing body or from the school's legal advisers where necessary.

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request

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:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- 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.

1.12 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 based on 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

1.13 Providing information

Step By Step school aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the school has a privacy statement, setting out how data relating to individuals is used by the school plus a GDPR statement on our web site. A more

detailed statement with regard to GDPR is available upon request from the Compliance.officer@stepbystep.org.uk if required.

1.14 Data protection by design and default

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

- Appointing a suitably qualified DPO, 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
- 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 DPO 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 DPO 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

1.15 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 paper-based records, and overwrite or delete electronic files. We also use a third party to safely dispose of records on the school's behalf, who provide guarantees that they comply with data protection law.

1.16 Training

All staff and governors are provided with data protection training as part of their induction process and via an online training course. Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

1.17 Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy, this policy will be reviewed **every 2 years** and shared with the full governing board.

2. Data Breaches

Step by Step school holds, processes and shares a large amount of personal data. This is an asset that needs to be suitably protected.

Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentially, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provisions, legislative non-compliance, and/or financial costs.

2.1 Purpose

Step by Step school is obliged under law to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place from managing data breach and information security incidents across the school.

2.2 Scope

This policy relates to all personal and sensitive data held by Step by Step school regardless of format.

This policy applies to all staff at the school. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of Step by Step.

This policy is effective as of the issue date and does not expire unless superseded by another policy.

2.3 Definitions

For the purpose of this policy, data security breaches included both confirmed and suspected incidents.

In case of an incident defined as “a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed” this policy will define the required actions to be taken when a breach is identified or suspected.

A data breach relates to the loss of personal data and should be notified following the procedure described within this policy. A security breach relates to the loss of equipment containing personal data. Where a security breach has been notified that also involves personal data staff must also follow the data breach policy.
An incident in the context of this policy is an event or action which may compromise the confidentially, integrity or availability of systems or data, either accidentally or deliberately. And has caused or has the potential to cause damage to Step By Step’s information assets and/or reputation.

An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which data is stored (e.g. loss of laptop, USB drive, iPad/tablet, phone or paper record)
- Equipment theft or failure

- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed and successful) to gain unauthorised access to information on IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attacking
- Unforeseen circumstances such as fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who hold it

The definition of a breach a breach of security leading

- to the accidental or unlawful destruction, loss, alteration,
- unauthorised disclosure of, or access to, personal data
- transmitted, stored or otherwise processed

2.4 Reporting an incident

Any individual who accesses, uses or manages Step by Step's information is responsible for reporting data breach and information security incidents immediately to their line manager and the IT Help desk so that a ticket can be raised.

If the breach occurs or is detected outside of normal working hours, it must be reported as soon as is practicable.

The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An incident report form should be completed as part of the reporting process. See Appendix 1.

All staff should be aware that any breach of the GDPR may result in Step by Step's disciplinary process being instigated.

2.5 Containment and Recovery

Focus IT will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken to minimise the effect of the breach. The IT help desk will appoint an Information Security Office (ISO) to assist in the investigation.

An initial assessment will be made by the ISO in liaison with relevant parties to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach in some cases it could be the ISO).

The appointed Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO will establish who needs to be notified as part of the initial containment and will inform the authorities (including the police if necessary) where appropriate.

Advice from experts across Focus Group (or other IT suppliers) may be sought in resolving the incident promptly.

The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

2.6 Investigation and Risk Assessment

An investigation will be undertaken by the LIO immediately and wherever possible within 24 hours of the breach being discovered / reported.

The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences to the individual, how serious or substantial those are and how likely they are to occur.

The investigation will need to consider the following:

- The type of data involved.
- Its sensitivity.
- The protections that are in place (e.g. encryption).

- What's happening to the data, has it been lost or stolen?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- Would notification help Step by Step school meet its obligation under the seventh data protection principle? (Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data).
- If a large number of people are affected, **or** there are serious consequences, whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved. Guidance on when and how to notify ICO is available from their website at https://ico.org.uk/media/1536/breach_reporting.pdf
- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquires and work.

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact Step by Step school for further information or to ask questions on what has occurred.

The LIO and or the ISO must consider notifying third parties such as the police, insurers, bank or credit companies. This would be appropriate where illegal activity is known or believed to have occurred, or where there is a risk that illegal activity may occur in the future.

2.7 Evaluation and Response

Once the initial incident is contained, the ISO will carry out a full review (Root Cause Analysis – RCA) of the causes of the breach, the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amounts of data necessary
- Identifying weak points within existing security measures
- Staff awareness
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by the Governing body.

2.8 Enforcement

Handling and recovering from data breaches is important to security and confidentiality of systems and data, employees that purposely violate this policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal. Any member of staff aware of any violation of this policy is required to report it to their supervisor or other authorised representative.

Appendix 1 – Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach, please notify your line or departmental manager immediately. Complete section 1 of this form and email to the Information Security officer and the Help desk.

Data Breach Report Template v1.0.docx

EXTERNAL LINKS

Reference	Description	Link
1.0	Link to the 99 articles that define the GDPR	General Data Protection Regulation (GDPR)
1.1	Data protection bill	Data Protection Bill
1.2	Handling Subject Access Request	Code of practice for subject access requests