Data Protection Policy

The Edith Borthwick School

October 2021 – Plus Appendix A - Data Security – Protocols and Guidance for Staff

sbm services
school business management

Date Staff Consulted	**N/A**
Lead Governor	**Ruth Sturdy**
Date approved by Resources Committee	**4.2.22**
Date approved by Governing Body	**N/A**
Next review date	**Spring 2024**

Contents

Part 1 Introduction and Key Definitions

1.1 Introduction

The Edith Borthwick School needs to gather and use certain information about individuals.

These individuals can include pupils, parents/carers, employees, 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 school's data protection standards — and to comply with the law.

This data protection policy ensures The Edith Borthwick School:

- complies with data protection law and follows good practice
- protects the rights of pupils, staff, parents/carers and other stakeholders
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

This data protection policy is based on the six principles of the Data Protection Act (DPA) that personal data shall be:

1. processed lawfully, fairly and in a transparent manner
2. collected for specified, explicit and legitimate purposes
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. accurate and kept up to date
5. kept in a form which permits identification of data subjects for no longer than is necessary
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss or damage

1.2 Key Definitions

Data

The DPA describes how organisations, including The Edith Borthwick School, must collect, handle and store personal information ('data').

Data is any information that the school collects and stores about individuals or organisations. Some data is more sensitive than others and particular care will be given to processing and managing this. Sensitive data includes:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;

- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data; and
- biometric data.

Data can be 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.

Data Subject

A 'Data Subject' is someone whose details the school/academy keeps on file. The data subject has the following rights under data protection legislation:

- to be informed
- to have access to data stored about them (or their children)
- to rectification if there is an error in the data stored
- to erasure if there is no longer a need for the school to keep their data
- to restrict processing (e.g. limit what their data is used for)
- to object to data being shared or collected

Although data protection legislation affords these rights to individuals, in some cases the obligations schools have to share data with the DfE etc override these rights (this is documented later in the policy under 'Privacy Notices').

Data Controller

The 'Data Controller' has overall responsibility for the personal data collected and processed and has a responsibility for ensuring compliance with the relevant legislation. They are able to delegate this to 'Data Processors' to act on their behalf.

The Edith Borthwick School is the 'Data Controller'.

Data Processor

A 'Data Processor' uses, collects, accesses or amends the data that the controller is authorised to collect or has already collected. It can be a member of staff, third party company or another organisation such as the police or Local Authority (LA).

Part 2 Organisational Arrangements

2.1 Overall Responsibility

The Edith Borthwick School will meet its obligations under the DPA by putting in place clear policies that focus on the key risks and in checking that control measures have been implemented and remain appropriate and effective.

2.2 Roles & Responsibilities

Each school/academy may have different arrangements in place for these roles and responsibilities.

If a section is not relevant to your setting then delete it accordingly. Likewise additional sections can be added if appropriate to your setting. These are just suggestions for inclusion within your policy.

The Governing Body will:

- Establish and maintain a positive data protection culture.
- Ensure the Headteacher prepares a Data Protection policy for approval and adoption by the Governing Body and to review and monitor the effectiveness of the policy.
- Appoint a Data Protection Officer and provide adequate resources and support for them to fulfil their statutory duties.
- Allocate sufficient resources for data protection, e.g. in respect of training for staff, encryption technology for devices.
- Monitor and review data protection issues.
- Ensure that the school provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their data protection responsibilities.
- Review and act upon data protection compliance reports from the Data Protection Officer.

The Headteacher will:

- Promote a positive data protection culture.
- Prepare a Data Protection Policy for approval by the Governing Body, revise as necessary and review on a regular basis, at least every two years.
- Ensure that all staff cooperate with the policy.
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training.
- Provide staff with equipment and resources to enable them to protect the data that they are processing.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.
- Monitor the work of the Data Protection Officer to ensure they are fulfilling their responsibilities.

The Data Protection Officer will:

- Inform and advise the school of their obligations under data protection legislation.
- Monitor compliance with the legislation and report to the Headteacher and Governing Body on a termly basis.
- Cooperate with the supervisory authority (e.g. Information Commissioners Office) and act as the main contact point for any issues.
- Seek advice from other organisations or professionals, such as the Information Commissioners Office as and when necessary.
- Keep up to date with new developments in data protection issues for schools.
- Act upon information and advice on data protection and circulate to staff and governors.
- Carry out a data protection induction for all staff and keep records of that induction.
- Coordinate the school response to a Subject Access Request.
- Coordinate the school response to a data breach.

Staff at the school will:

- Familiarise themselves and comply with the Data Protection Policy.
- Comply with the school data protection arrangements.
- Follow the data breach reporting process.
- Attend data protection training as organised by the school.

Part 3 Detailed Arrangements & Procedures

Each school/academy will have different arrangements in place for these sections therefore these need to be personalised to reflect your own organisational arrangements.

If a section is not relevant to your setting then delete it accordingly. Likewise additional sections can be added if appropriate to your setting. These are just suggestions for inclusion within your policy.

3.1 Data Management

Data Registration

As Data Controller, the school must register as a Data Controller on the Data Protection Register held by the Information Commissioner. The school was last registered on 16/05/05 and is due to renew on 15/05/22.

Data Protection Officer

As a public body, The Edith Borthwick School is required to appoint a Data Protection Officer (DPO).

At The Edith Borthwick School the DPO role is fulfilled by:

- SBM Services Ltd

The role of the DPO is to:

- Inform and advise the school/academy and the employees about obligations to comply with all relevant data protection laws.
- Monitor compliance with the relevant data protection laws.
- Be the first point of contact for supervisory authorities.
- Coordinate training on data protection for all key stakeholders in the school.

Data Protection Awareness

In order to ensure organisational compliance, all staff and other key stakeholders (e.g. governors, volunteers) will be made aware of their responsibilities under the data protection legislation as part of their induction programme, (both as a new employee/governor to the organisation or if an individual changes role within the school/academy).

Annual data protection refresher training will take place to reinforce the importance of staff adhering to the legislation.

A record of the professional development undertaken by the individual will be retained on their training record.

Data Mapping

The Edith Borthwick School has documented all of the data that it collects within a 'Data Flow Map'. This data inventory records:

- the data held
- what the data is used for
- how it is collected
- how consent is obtained
- how the data is stored
- what the retention period is
- who can access the data
- who is accountable for the data
- how the data is shared
- how the data is destroyed

For each data type, the probability of a data breach occurring is assessed (very high, high, medium, low or very low) and actions to be taken to mitigate the risk are recorded.

It is the responsibility of the DPO to ensure the 'Data Flow Map' is kept up to date. The map should be a live document and updated regularly.

3.2 Third Party Suppliers Acting as Data Processors

As Data Controller, the school is responsible for ensuring that correct protocols and agreements are in place to ensure that personal data is processed by all subcontractors and other third parties in line with the principles of the data protection legislation.

Individuals within school who have a responsibility for securing contracts and agreements with such third parties are responsible for ensuring that all external data processing is contracted out in line with the principles of the DPA. These type of agreements include:-

- IT contracts and processes.
- Physical data and hard copy documents.
- Data destruction and hardware renewal and recycling financial and personnel information.
- Pupil and staff records.

Only third-party suppliers who can confirm they have appropriate technical, physical and organisational security to securely process data will be considered as suitable partners.

The procurement process will ensure that all contracts are suitable and reflect DPA requirements. Review of current and due consideration of future contracts will require this even if data processing is ancillary to the main purpose of the contract.

The external processor will confirm with the data controller that suitable security and operational measures are in place.

Any potential supplier or purchaser outside the EU will be obliged to confirm how they comply with the DPA and give contractual assurances.

The DPO may require a specific risk assessment to be undertaken if the data is sensitive, and if an increased risk is likely due to the nature, or proposed nature, of the processing.

A written agreement will be in place between the supplier and the school to confirm compliance with the DPA principles and obligations to assist the school in the event of a data breach or subject access request, or enquiries from the ICO.

The school must have the right conduct audits or have information about audits that have taken place in respect of the relevant processes of the supplier's security arrangements whilst the contract is in place, or whilst the supplier continues to have personal data that relates to the contract on its systems.

Any subcontracting must only be done with the written consent of the school as data controller. This must be the case for any further subcontracting down the chain. All subcontractors must confirm agreement to be bound by DPA principles when handling the school's data, which shall also include cooperation and eventual secure destruction or return of data.

The school has a 'Third Party Request for Information' form which must be used for third-party suppliers acting as a Data Processor for the school.

3.3 Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases, data will only be processed if explicit consent has been obtained.

Consent is defined by the DPA as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

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

Privacy Notices

In order to comply with the fair processing requirements of the DPA, the school will inform their staff and parents/carers of all pupils of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc) to whom their data may be passed, through the use of 'Privacy Notices'.

Privacy notices are available to staff and parents through the following means:

- School website
- School prospectus
- Staff Handbook
- Staff Notice Boards

The Use of Pupil Images

Occasionally the school may take photographs of its pupils. These images could be used as part of internal displays, printed publications, the school website or our social media accounts.

The Edith Borthwick School will seek consent from all parents to allow the photography of pupils and the subsequent reproduction of these images. Consent will be sought on an annual basis.

Parents are given the opportunity to opt in. It is not permissible to assume parents are opting in.

Generic consent for all uses of images is not acceptable; parents must give consent to each medium.

Parents must be given the opportunity to withdraw their consent at any time. This should be given in writing to the school, however a verbal withdrawal of consent is also valid and should be reported to The School Business Manager immediately.

Consent should be recorded onto SIMS and a word document should be maintained for each class that details each individual consent given. This is a living document and should be updated by the Receptionist when any new consents are given or when a 'Withdrawal of Consent' form is received.

If images of individual pupils are published, then the name of that child should not be used in the accompanying text or caption unless specific consent has been obtained from the parent prior to publication.

The school 'Parental Consent' form should be issued to current parents to seek consent annually.

Accurate Data

The school will endeavour to ensure that the data it stores is accurate and up to date.

When a pupil or member of staff joins the school they will be asked to complete a form providing their personal contact information (e.g. name, address, phone number, NI number for staff), next of kin details, emergency contact and other essential information. At this point, the school will also seek consent to use the information provided for other internal purposes (such as promoting school events, photography).

The school will undertake an annual data collection exercise, where current staff and parents will be asked to check the data that is held about them is correct. This exercise will also provide individuals with the opportunity to review the consent they have given for the school to use the information held for internal purposes.

Parents/carers and staff are requested to inform the school when their personal information changes.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, the school will consider each situation on its merits and within the principles of the DPA, child welfare, protection and safeguarding principles.

Parents/carers and staff are requested to complete a Withdrawal of Consent form and return this to the Receptionist.

3.4 Associated Data Protection Policies

- CCTV
- Complaints
- Data Breaches
- Records Management
- Subject Access Requests
- Third Party Requests for Information
- Use of Personal Devices
- IT Useage

CCTV

The Edith Borthwick School uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to the school property. The school has a CCTV Policy in place which documents:

- why CCTV is used
- where cameras are sited
- whether covert monitoring is undertaken
- how long images are retained for
- who has access to the images
- what the complaints procedure is

Complaints

Complaints will be dealt with in accordance with the school's Complaints Procedure. An individual may contact the Information Commissioner's Office (ICO) if they are not satisfied with how a complaint has been dealt with by the school. The telephone number for the ICO is 0303 123 1113.

Data Breaches

Although the school takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space).
- Unforeseen circumstances such as fire or flood.
- Hacking attack.
- ‘Blagging’ offences where information is obtained by deceiving the school.

The school has a Data Breach Policy which sets out the process that should be followed in the event of a data breach occurring.

Privacy Impact Assessments

When considering the purchase of a new service or product that involves processing personal data, a Data Privacy Impact Assessment must be completed by the DPO. If risks are identified as part of the assessment then appropriate steps to mitigate this risk must be implemented. If these risks are deemed to be ‘high risk’ then the DPO should consult with the ICO prior to implementation.

The ‘Data Privacy Impact Assessment’ form must be used for each new service/product.

Records Management

The school recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations which will also contribute to the effective overall management of the school.

The school has a Record Management & Retention Policy in place which sets out how it will:

- safely and securely store data (both digital and hard copy data)
- retain data
- dispose of data

Subject Access Requests

Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the school/academy holds about them, and can make a Subject Access Request (SAR).

The school has a Subject Access Request Policy, which sets out the process that should be followed in the event of receiving a SAR.

Third Party Requests for Information

Occasionally the school may receive a request for information on a pupil or member of staff by a third party, such as the police or social services. This would be separate to statutory requests that come through from the DfE or LA, for example, which are covered within the privacy notices.

The school has a Third Party Request for Information Policy which sets out the process that should be followed in the event of receiving a third party request.

Use of Personal Devices

The school recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices. The school follows the ‘Bring Your Own Device’ Policy which sets out how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school.

Data Protection Policy - APPENDIX A

Data Security - Protocols and Guidance for Staff

The school aims to keep data safe and secure at all times acknowledging issues of confidentiality, data protection, and rights of access. We aim to build upon industry standard practice and work with operational solutions that will minimise risk and comply with current legislation.

The risk of data being lost or stolen is encountered on a day to day basis and we seek to ensure that we are vigilant in order that we first and foremost do not cause individuals or families harm or distress, and secondly cause an organisational issue that would undermine the school reputation and confidence in our systems.

The guidance given in this document may necessitate changes to your work practices. However, the protocols do give an expected course of action to follow that is both safe and effective, and designed to safeguard all staff; you should therefore adhere to them in your ongoing work with data.

What constitutes data?

The Information Commissioners Office supplies the following generalised definitions:

Data means information which –

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

Personal data means data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive personal data means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The Data Protection Act regulates activities relating to data.

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

Your roles and responsibilities as a member of staff

If you encounter or use personal data during your employment you have a responsibility both individual and collective to ensure that it is maintained and passed on in a secure and efficient manner. Please make sure that the following points are acknowledged and met:

- Make sure you and your colleagues are adequately trained and inform senior managers if you require Continuing Professional Development.
- Follow Protocols and Guidance at all times.
- Become more data security aware.
- Be aware of the sensitivity of the data that you are working with and passing on.
- Raise any security concerns with the Network Manager, Technician or Headteacher.
- Encourage your colleagues to follow good practice.
- Report any incident or concern - however trivial.

Information to protect

You are required to secure and keep safe any personal data that is deemed sensitive or otherwise valuable to the school. Please see the Data Protection Policy for more information.

Protective Markings

Some information may have protective markings and/or be marked confidential. In this case you should be aware of who can view the information.

Preventing Security Problems

Working online

Do:

- Make sure that you follow the school policies, including E-Safety, Data Protection and Personal Mobile Devices.
- The school updates virus scanners and associated security software, if you think that your laptop or desktop machine has taken a hit with a virus inform the Network Manager or Technician immediately.
- It is not good practice to transfer files between home and school using external devices, e.g. memory sticks and SD cards. Sensitive data, as defined in the Data Protection policy, must never be transferred in this manner.
- Only visit websites that are allowed in school. The school has filters and also monitors the use of the school computer network including individual websites.
- Make use of security settings within the web browser. These will usually have been enabled when your hardware is set up.
- Make sure that all software is known and approved by the school. Conflicts are common between versions of the same programme.
- Be very wary of game sites or links to websites in emails.
- Only download programmes from a source that you know and trust. Check with the Network Manager or Technician if in doubt.

Email

Best Practice:

- Keep your mail boxes maintained and remove unwanted or outdated files.
- Inform the Network Manager if you receive spam or unwanted unsolicited mail.
- Be aware of who you are sending the mail to – once it is sent it cannot be retrieved.
- Report any data breaches by email to the Data Protection officer.
- Be wary and do not open unsolicited mail – it may carry a virus.
- Never share sensitive data via unencrypted email – Discuss with the Network Manager if in doubt.
- Share secure information over the school network rather than via email.

Passwords

Do:

- Keep them personal – do not share with anyone.
- Use a strong password - 8 characters minimum upper and lower case letters plus a number.
- Make it easy to remember but hard to guess.
- Use a rhyme or phrase to help you remember. Change and/or reset your password if it has been discovered. Discuss with the Network Manager.
- Update your password on a regular basis (every 3 months)
- When using Apple devices, please use a unique 6 digit password and finger print.
- Have unique passwords for each application used.

Don't:

- Keep a written password on display.
- Share it with anyone else.
- Use a school password for your own personal use.
- Save passwords in web browsers.
- Use your username as a password.
- Email your password.
- Keep your password at default settings.

Use of Laptops

Do:

- Lock your computer prior to making a temporary absence.
- Shut down your laptop after use using 'shut down'.
- Turn off and store your laptop securely. Use the transport bag to store when not in use.
- Store your documents in the Documents file.
- Use the appropriate desktop at all times - staff or student.
- Confirm that the synchronisation process is backing up your data on the server. This should be undertaken on a regular basis, at the very least weekly.

Don't:

- Leave your computer logged on and unattended.
- Use standby instead or turning it off.
- Use your on screen desktop as a documents repository.
- Let anyone else use your logon or change the security settings.
- Install unauthorised software.
- Leave your laptop unattended unless you are sure of building security
- Leave it on display in a car - lock it in the boot.
- Leave it unattended in a public place.
- Use public wi-fi hotspots – they are not secure, leaving you vulnerable to being hacked.

Use of External Storage, e.g. Memory Sticks and Cards

The use of external storage, e.g. memory sticks is fraught with risks and difficulties. The widespread passing of substantial and significant information with memory stick or SD card is not encouraged, and in such instances staff should use the secure networked server provision in school or a school cloud service. Do not use these devices as backup storage. Whilst such devices may be convenient they are far from secure, transmit viruses from one machine to another, and are easily lost, stolen, or corrupted. Use them with the utmost care and discretion – see below. Under no circumstances may any sensitive data, as described in the Data Protection Policy be transferred or transported using external storage.

Sending and Sharing Information

Do:

- Be aware of what information you are sharing, and with whom you are allowed to share it. Check with the Headteacher or School Business Manager.

Don't:

- Pass sensitive information on removable media.
- Make assumptions that information passed to other people will be maintained in a safe and efficient way.

Working on site

Do:

- Do lock sensitive information away when it is unattended – turn off or lock your computer.
- Keep your laptop turned off and bagged when not in use.

Don't:

- Let unauthorised people including parents into staff areas.
- Position screens where they can be read by other people, including those outside the room.

Working off site

Do:

- Only take information off site if you are authorised and it is necessary to do so. Consult with the Headteacher or School Business Manager if in doubt.
- Where possible access data from the server.
- Be aware of your location and the data you are handling – then take all reasonable steps to mitigate risk.
- Sign out from any secure sites you have been using.
- Reduce the risk of people viewing what you are working with.

- Do not take your laptop abroad, all school data should remain within the UK – some countries prohibit encryption technologies.

The school has a legal obligation under the 2018 General Data Protections Regulations (GDPR) to ensure that all personal information and data relating to staff and pupils is maintained and held in an effective and safe manner, and these protocols and guidance support that process. For further information you may consult www.ico.gov.uk.

These protocols and guidance points will be reviewed annually and updated as required.