Data Protection (GDPR) Policy

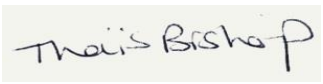
Issue Date: July 2018, July 2020

Review Date: This policy will be reviewed and revised by the administration team on a biennial basis.

Endorsement: Full endorsement to this policy is given by:

Name: Thais Bishop

Position: Brighton Waldorf School Trustee

Signed: 

Review Date: July 2022

1. Introduction

BRIGHTON WALDORF SCHOOL (the School) collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the school to provide education and other related services. There is also a legal requirement for schools to collect and use information to ensure that the school complies with its statutory obligations.

2. Definitions

Data Protection legislation places obligations on all those who process personal data and defines the following roles:-

Data Controller – the person or organisation that determines the purpose of processing i.e. decides how and why data is used. The school is therefore a data controller.

Data Processors – the person or organisation that processes data on behalf of the controller. The school is sometimes a data processor.

Data Subjects – the individuals whose information is collected and processed (for example pupils. parents, carers, members of staff)

ICO – Information Commissioner's Office

3. Registration

BRIGHTON WALDORF SCHOOL, as a data controller, have to register with the Information Commissioner's Office and maintain a record of the information it holds and the purposes for which it obtains and uses personal data (including disclosure in any form to third parties). These details must be kept up to date and be available for inspection by the Information Commissioner's Office.

4. The Information Commissioner

The Information Commissioner is the body that oversees compliance with Data Protection legislation, and has powers to force organisations to process personal data lawfully.

Where a data subject is unhappy with some aspect of the processing of their personal information they have the right to complain to the Information Commissioner.

It is recommended that any such issue should be resolved locally between the school and the individual concerned where possible. Any enquiries subsequently received from the Information Commissioner will be referred to the school's Data Protection Officer.

5. Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with Data Protection and other related legislation. It applies to information held and processed by the school regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities and will be required to comply with this policy.

6. Policy Statement:

BRIGHTON WALDORF SCHOOL is committed to ensuring that all information is collected, processed, maintained and disclosed in accordance with the principles that personal data will be:

- processed lawfully, fairly and in a transparent manner
- collected and used for specified, explicit and legitimate purposes and not further processed in an incompatible way ('*purpose limitation*')
- adequate, relevant and limited to what is necessary for the purpose for processing ('*data minimisation*')

- accurate and where required, rectified without delay ('*accuracy*')
- not be kept in an identifiable form for longer than necessary ('*storage limitation'*) i.e. in line with the school's retention schedule
- Information must be appropriately secured/protected against unauthorised or unlawful processing, accidental loss, destruction or damage using appropriate technical or organisational measures ('*integrity and confidentiality'*). This includes:
    - *using appropriate means of transmitting data*
    - *secure storage / disposal of personal information*
    - *where processing is sub-contracted or outsourced (e.g. payroll, disposal of confidential waste paper) there must be suitable Data Protection clauses in the contract*

See the school's Information Security Policy for more information on securing personal data (see section 14).

Personal information must also:

- be processed in accordance with the rights of data subjects e.g. right of access, right of erasure, rectification, restriction, portability and the right to object to certain processing (see section 12)
- not be transferred to countries outside the European Economic Area without adequate protection

6.1. 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 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).

6.2 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.

7. General Statement

Brighton Waldorf School is committed to maintaining the above principles at all times. Therefore **Brighton Waldorf School** will:

- Inform individuals why the information is being collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely in accordance with the School's retention schedule
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

8. Responsibilities

All employees, Trustees and any other individuals handling personal information on behalf of the school have a responsibility to ensure that they comply with Data Protection legislation and the school's policies.

The Trustees has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

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 Trustee Board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the main point of contact for individuals whose data the school processes for subject access requests or data breach notification, and for the ICO.

The School Director is the data controller on a day-to-day basis.

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 or not they have a lawful basis to use personal data in a particular 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

The school will ensure that all staff who are involved in processing personal data complete the school's data protection training.

9. The Legal Basis

The school must comply with all relevant UK and European Union legislation, including:

- Human Rights Act 1998
- Data Protection Legislation (Data Protection Act 1998, GDPR, Data Protection Act 2018)
- Freedom of Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Health and Safety at Work Act 1974
- Privacy and Electronic Communications (EC Directive) Regulations 2003

This Policy is also 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.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

10.Information and Data Definitions

Information is the product of a collection of data and expressed views and opinions based upon it. It can be held and used in many forms including, but not limited to, electronic records, hard copy (paper, fiche) phone calls and conversations. For the purpose of this policy, information and data can be regarded as being the same.

This policy relates primarily to any personal data i.e. data relating to individuals or personally identifiable data

- **Personally Identifiable data** is any data relating to an individual ('data subject) who can be identified directly or indirectly by an identifier such as name, ID number, unique pupil number, location data (e.g. address), online identifier (e.g. IP address) or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

- **Special Category Data** is sensitive personal data (which requires extra protection) and includes any information that may identify an individual's:

    - racial or ethnic origin,
    - political opinions,
    - religious or philosophical beliefs,
    - trade union membership,
    - health,
    - sex life/orientation
    - genetic/biometric identifier

Information that is **confidential** but doesn't relate to an individual or individuals includes the following:

- School business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information

- Information relating to security, investigations and proceedings
- Any information which, if released, could cause problems or damage to individuals, the public, the school or another organisation. This could be personal, financial, reputation or legal damage.

11. CCTV

We currently do not use recorded CCTV in our school site.

12. 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.

We will obtain written consent from parents/carers, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

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.

See our **Images Policy** for more information on our use of photographs and videos.

13. Data Protection by Design

Whenever a new policy, procedure, system or database involving personal data is proposed a Privacy Impact Assessment will be completed. This will be used to identify and reduce any risks to privacy and potential risks of harm to individuals through the misuse of their personal information.

14.Data Subject Rights (Subject Access Requests)

Any person wishing to exercise their rights under data protection legislation can do so by making 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 using our **Subject Access Request Form** (See Appendix 3) at the end of this policy. A hard copy is obtainable from the school office. Completed Subject Access Request Forms should be returned to the School Office so they can be forwarded to the DPO.

All Subject Access Requests must include:

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

When school staff receive a subject access request they must immediately forward it to the DPO.

Requests will be processed within 1 month of receipt of the request unless the request is complex (or if multiple requests are received from the same person)

Examples of when a request may be considered complex:

- it involves retrieval and appraisal of information from multiple sources
- it involves the retrieval of large volumes of information for one data subject which are difficult to separate from information relating to other data subjects
- it is one in a series of requests from the same individual
- it involves the release of third party data for which consent has been refused or cannot be obtained

In these cases a 3 month deadline for responding to the request will apply. For complex requests likely to take over 1 month, the applicant will be notified of this within the initial 1 month period.

Right of Access

Under data protection legislation every individual has the right of access to information relating to them. This right is called Subject Access. Any person wishing to make a Subject Access request can do so by following the instructions above. Personal information will never be disclosed verbally in response to a request.

Written consent will always be required from any person nominating a third party to request information on their behalf. Parents may make requests on behalf of their children but if the child is 13 years or older, the child must also provide written consent for the parent to make the application on their behalf.

A nominated person may make an application on behalf of anyone lacking mental capacity who would otherwise have the right to request access to their records. In these circumstances, the person making the application must have proof of a valid Lasting Power of Attorney or an Enduring Power of Attorney or proof of Court-appointed Deputyship.

No information relating to any other person (other than the individual requesting the information) will be disclosed as part of a subject access disclosure.

Any information that may prejudice the prevention and detection of crime may be exempt from disclosure. There are also a number of other exemptions which may be applied and these will be explained on an individual basis.

Right of erasure

This right allows individuals to request that their personal data is deleted where there is no justification for its continued use. It only applies, however, when:

1. The data is no longer necessary for the reason(s) for which it was originally collected
2. The data subject provided consent for the school to process their data but has subsequently withdrawn this consent
3. That data subject has objected to the school processing their data and there are no overriding grounds for continuing to process it
4. The data was processed in breach of the GDPR i.e. it was unlawfully processed
5. There is a legal requirement to erase the data
6. The data was collected with parental consent when the data subject was a child and they no longer wish for their data to be held

The school will also decline a request for erasure:

1. When we have a legal obligation or it is part of our official authority to process the data
2. For public health reasons
3. For certain archiving activities
4. When we need the data in connection with a legal claim

Right to rectification

If data subjects believe that any of the personal data the school holds about them is inaccurate or incomplete they are entitled to ask for it to be rectified. This will be looked at in the context of why the school is processing the information. Any necessary steps will be taken to supplement the information held in order to make it complete.

Right to restriction

In certain circumstances data subjects have a right to request that we temporarily restrict processing and access to their data. This will apply:

1. Whilst establishing accuracy of data, if a data subject has contested this
2. Whilst we follow up any objection raised by a data subject to the school processing their data.
3. When data has been processed unlawfully but the data subject does not want us to erase it and have asked, instead, for us to restrict processing of the data.
4. When we no longer need the data but the data subject has advised us that they need it in connection with a legal claim.

The right to restrict data doesn't apply if:

1. The processing is necessary for the school in connection with a legal claim
2. It is necessary for the protection of another person
3. There are substantial public interest reasons for continuing to process the data

Right to portability

Data subjects have a right to request that their data be transferred electronically to another organisation.

This only applies when:

1. The data subject themselves supplied the information and provided consent for the processing; or
2. The data is being processed as part of a contract to which the data subject is party; and
3. The data is held electronically (not in paper files)

Right to object

Data subjects have the right to object to their information being processed in the following circumstances:

- If the school has decided that processing is necessary either to

a) Perform a task carried out in the public interest or

b) As part of the school's official authority or legitimate interest and the data subject feels this is not applicable.

Information about why the school is processing information (the legal justification) can be found in the school's privacy notice.

- If the school retains information in defence or potential defence of a legal claim but the data subject believes there are insufficient grounds to do so.

Data subjects also have a right to object to their data being used for direct marketing purposes at any time and the school will cease processing for this purpose if an objection is raised.

If the school uses IT systems to make automatic decisions based on personal data individuals have a right to object and:

- request human intervention in the decision making
- be able to express their point of view
- obtain an explanation of how a decision has been reached
- challenge the decision

This right does not exist if the automated decision making:

- is necessary to fulfil a contract to which they are party
- is authorised by law
- the data subject has consented to the processing

Individuals also have the right to object to data being used for research purposes unless the research is being undertaken in the wider public interest which outweighs a data subject's right to privacy.

Right to be Informed

The school issues a privacy notice which explains what information the school is processing, the legal basis for this, the purpose of processing, who the information is shared with and other information required by data protection legislation. The current privacy notice is available on the school's website (www.brightonWaldorfschool.org.uk)or on request from the School Office in person or by e mail (see Section 19).

15.Breaches of Data Protection

The school has a data breach management process (see Appendix 1) which all staff are aware of and have received appropriate training to help them recognise and react appropriately to data breaches.

Such breaches in a school context by way of example could include, but are not limited to:

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

All breaches or suspected breaches of Data Protection legislation will be reported to the school's Data Protection Officer who will ensure the process is adhered to and ensure breaches are reported to the ICO where necessary.

16.Information security

The school's Information Security Policy covers the creation, acquisition, retention, transit, use, and disposal of all forms of information.

It applies to all employees and School Trustees; it also applies to volunteers, work experience candidates, and all staff of service delivery partners and other organisations who handle information for which the school is responsible. It will form the basis of contractual responsibilities in contracts with Data Processors where reference is made to the school's Data Protection and Information Security Policy.

It is the policy of the School that:

- we will protect information from a loss of:

  - confidentiality (ensuring that information is accessible only to authorised individuals)
  - integrity (safeguarding the accuracy and completeness of information)
  - availability (ensuring that authorised users have access to relevant information when required)
  - relevance (only keeping what we need for as long as it is needed)
- we will meet all regulatory and legislative information management requirements
- we will maintain business continuity plans
- we will deliver appropriate information security training to all staff
- we will make available appropriate and secure tools to all staff
- we will report and follow-up all breaches of information security, actual or suspected

Guidance and procedures will be maintained to support this policy. These will include procedural standards for individuals with access to information.

System operating procedures will be developed and maintained to ensure compliance with this policy.

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 sign it in and out from the school office
- 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 is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [online safety policy/ICT policy/acceptable use agreement/policy on acceptable use])

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

17. Management of Information

The School will manage information in accordance with the principles and procedures within this policy and other relevant policies and standards. The following principles apply to how we handle information in the school:

- All identifiable personal information is treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- Procedures will be maintained to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information is recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

18. School records

We will create and maintain adequate pupil, staff and other records to meet the school's business needs and to account fully and transparently for all actions and decisions. Such records can be used to provide credible and authoritative evidence where required; protect legal and other rights of the school, its staff and those who have dealings with the school; facilitate audit; and fulfil the school's legal and statutory obligations.

Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner, in line with the school's Records Management and Electronic Records Management policies.

19.Contacts

Data Protection Officer:

The appointed Data Protection Officer for Brighton Waldorf School is the School Director:

Phone: 01273 386300

School Contacts:

The School Office
Brighton Waldorf School
Roedean Road
Brighton

BN2 5RA

Email: admin@brightonWaldorfschool.org.uk

Office of the Information Commissioner:

The Information Commissioners
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Website: www.ico.gov.uk
Tel. 03031 231113

20. Monitoring arrangements

The DPO advises the Trustees who are responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the Board of Trustees.
Note: While the GDPR and Data Protection Act 2018 (when in place) are still new and schools are working out how best to implement them, you may wish to review your data protection policy annually, and then extend this to every 2 years once you are confident with your arrangements.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online Safety Policy
- Acceptable Use of ICT Agreements
- Safeguarding and Child Protection Policy
- Images Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPO will alert the School Director, Chair of College and the Chair of Trustees

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them

any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system in a restricted access drive.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach

  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's computer system in a restricted access drive.

- The DPO, School Director and Chair of College will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Implementation

The School Director/DPO 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 DPO, School Director or the Chair of College.

Appendix 2: Data Breach Record

Data Protection Breach Record

Date:_____/_____/_____	**Person Responsible for dealing with Breach:_____**
Breach Description	
Which Data Subjects are involved	
Personal Data type involved	

Number of Personal Data Records affected					
Breach Reported by					
Likely consequences of Data Breach					
Phone/e-mail sent to DPO	**Y / N**	**Is this High Risk?**	**Y / N**	**Report to ICO?**	**Y / N**
Date reported to the Data Subject / Subjects	_____/_____/_____				
Remedial Actions taken (include date for each action)					
Preventative Action Suggestions – including training					
Notes					
Actions Approved by			**Date**	_____/_____/_____	

Appendix 3: Subject Access Request Form

Brighton Waldorf School
Roedean Road
Brighton
BN2 5RA

Email: admin@brightonWaldorfschool.org.uk

Re: Subject Access Request

Dear

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a free to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. Below are some examples of actions that could be taken. We will review the effectiveness of these actions and amend them as necessary after any data breach. In the event of any breach, our DPO will provide advice and support with all actions required.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Details of pupil information for named children (or similar types of personal data) being published on the school website

- If special category data (sensitive information) is accidentally made available via the School Website, the discoverer must alert the School Director or another School Leadership Team (SLT) member or Website Administrators, to remove the data immediately and alert the DPO
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- The DPO will work with the School Director and Chair of College to review who has access to edit the website and how personal data was published in this case. The review will consider access control for the website and the review of all data prior to publishing on the website by a member of the SLT.

A school laptop, hard disc drive or USB drive containing non-encrypted sensitive personal data being stolen or hacked

- Laptop / Drive holder to immediately alert the DPO and School Director
- DPO / School Director to identify the nature and scope of the data involved, through employee interview, searches of e-mail / back up archives and any other action necessary
- DPO to provide advice to School Director/ SLT on implications of potential data breach.
- DPO to work with School Director to establish if device user should be subject to a staff disciplinary procedure
- DPO to work with School Director, IT Network Manager and wider SLT to review device data security and ensure that all employees are aware of the Data Protection and Acceptable Use Policies.
- Audit of all establishment portable devices to be undertaken (Laptops / Tablet Devices / Portable Hard Disc Drives and USB Drives to establish that they are all password protected and all data is encrypted. All devices to be checked for sensitive personal data. Non-compliant devices to be withdrawn from use and replaced by compliant devices.
- In the case of a Hack, the DPO must report this to Action Fraud UK. SLT to work with the School Administration and ICT Consultants to improve device / network security to reduce the likelihood of a reoccurrence.

Non-anonymised pupil data or staff pay information being shared with Trustees

- DPO / School Director to identify source of the data
- Member of Staff who provided the data to be subject to disciplinary procedure and to be given further Data Protection training with regard to personal data
- Clerk to Trustees to ensure that all documents are checked prior to Trustees having access to them and to alert the School Director to any personal data content before they are sent out.
- DPO to contact all Trustees to ensure that they delete the relevant document/s and / or return any hard copies to the School for secure destruction.

The school's cashless payment provider being hacked and parents' financial details stolen

- DPO to contact provider to establish data loss extent

- DPO to ensure the provider has contacted all parents to ensure that all parents are aware and should alert their bank / building society accordingly

- DPO to maintain contact with the provider to ensure an interim system is established

- DPO to maintain dialogue with provider during their investigation and to have reasonable assurance that any new or modified payment system is protected against a similar hacking

- School Director to review contract with provider at an appropriate time; if provider is deemed to be in breach of contract and has not taken sufficient or timely corrective action, it may be appropriate to re-tender the contract.