Title	Data Protection Policy
Associated Policies	• Safeguarding and Child Protection (TPO/HS/05) • Staff Records (TPO/STA/16) • Professional and Safe Conduct (TPO/STA/10) • Whistleblowing (TPO/STA/19) • CCTV (TPO/QA/04)

REVIEWED: September 2021 NEXT REVIEW: September 2023

1. Policy Statement

1.1 The Trust is committed to complying with the principals of the General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA). This protects personal privacy and upholds individual's rights and it applies to anyone who handles or has access to people's personal data.

1.2 **The Trust as the Data Controller** will comply with its obligations under the GDPR and the Data Protection Act (2018). The Trust is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

1.3 This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

1.4 This includes ensuring the following:

- Monitoring and oversight by the appropriate committee or Board
- Assigning responsibility to an individual within the Trust;
- Assigning a Data Protection Officer;
- Development and maintenance of a GDPR project;
- Ensuring that all staff are trained in data protection and take responsibility for the collection, processing, storage and destruction of data;
- A lawful basis for processing is documented for all processing activity;
- Principles relating to processing of personal data are adhered to;
- The rights of data subjects are respected;
- Risks to the rights of data subjects are assessed and mitigated for all large-scale and new processing;
- Regular independent reviews of processing activity and processing documentation are carried out;
- Organisational and technical measures are implemented to protect data;
- Data breaches impacting on the rights and freedoms of data subjects will be reported to the ICO.

1.5 The Trust will refer to documents and guidance from the Information Commissioner's Office (ICO) and the Department for Education (DfE) in relation to GDPR and data processing.

1.6 This policy does not form part of any employee's contract of employment and may be amended at any time.

2. Who does this policy apply to?

2.1 All staff and volunteers must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy in order to comply with its obligations under GDPR and the Data Protections Act (2018).

2.2 **The ICO as the Regulator** can impose substantial fines for breaches of GDPR and the Data Protection Act 2018 and other Data Protection legislation. Therefore, it is imperative that the Trust, all staff and the workforce comply with the legislation. The Data Protection Officer will be the principal point of contact with the ICO.

3. Who is responsible for carrying out this policy?

3.1 Everyone who works or volunteers for Brooke Weston Trust has some responsibility for ensuring that data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and the data protection principles.

3.2 The **Board of Directors** is ultimately responsible for ensuring that Brooke Weston Trust meets its legal obligations. The Strategic Delivery Group is responsible for implementing and monitoring the effectiveness of this policy.

3.3 The Trust shall maintain a **Data Protection Officer (DPO)** to represent the rights of data subjects. **Our DPO is Data Protection Education** and they can be contacted at dpo@dataprotection.education.

3.4 The **DPO, Data Protection Education** is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

3.5 The Trust shall ensure that the DPO is involved properly and in a timely manner, in all issues which relate to the protection of personal data.

3.6 The Trust shall support the DPO in performing the responsibilities outlined below by providing resources necessary to carry out those tasks and access to personal data and processing operations. The DPO shall maintain his or her expert knowledge.

3.7 The Trust shall ensure that the DPO does not receive any instructions regarding the exercise of their tasks. They shall not be dismissed or penalised by the controller or the processor for performing his tasks.

3.8 The DPO shall directly report to the highest management level of the organisation, as needed and report to the Board of Directors at least once a year.

3.9 Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under the regulations.

3.10 The DPO and the Data Protection Lead will be bound by confidentiality and must maintain data security by protecting the confidentiality**,** integrity and availability of all personal data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that only authorised users can access the personal data when they need it for authorised purposes.

3.11 The DPO shall have the following responsibilities:

- Review of all data processing activities (inventory / mapping);
- Conduct of regular health checks/audits and issue recommendations;
- Assist with data protection impact assessments and monitoring performance;
- Monitoring and advice relating to subject access requests and data breaches;
- Assist the Trust with the maintenance of records;
- Monitoring and advice relating to FOI and other information requests;
- Cooperation with, and acting as the contact point for the ICO, who are the supervisory authority in respect of all data protection matters;
- Act as the contact point for data subjects to deal with requests and complaints;
- Training of organisation staff and workforce.

4. What are the principles behind this policy?

4.1 To fulfil its responsibilities the Trust needs to gather and use certain information about individuals. These can include students, parents/carers, staff, volunteers, suppliers, business contacts and other people the Trust has a relationship with or may need to contact. This policy describes how this personal data is to be collected, stored and otherwise processed to meet the Trust's data protection standards and to comply with the law.

4.2 Anyone processing personal data must comply with the data protection principles. The Trust will comply and is committed to these principles in relation to any processing of personal data. The Data Protection principles provide that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** in relation to the data subject and their rights;
- **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;
- **Accurate and, where necessary, kept up to date;**
- **Kept in a form which permits identification of data subjects for no longer than is necessary**;
- **Processed in a manner that ensures appropriate security of the personal data**
- **Must NOT be transferred to people or organisations situated in other countries without adequate protection.**

4.3 The Trust supports the rights of data subjects (or the parents/carers of data subjects where data subjects are not able to demonstrate the capacity to understand their rights) in relation to data that is processed or stored about them, as follows:

- Right to fair and transparent processing;
- Right of access;
- Right of rectification;
- Right to erasure (the "right to be forgotten");
- The right to restrict processing;
- Right to be notified of erasure, rectification or restriction;
- Right of data portability;
- Right to object to processing;
- Right to object to processing for the purposes of direct marketing;
- Right to object to processing for scientific, historical or statistical purposes;

- Right to not be evaluated on the basis of automated processing;
- Right to withdraw consent at any time;
- Right to be notified about a data breach;
- Right to an effective judicial remedy against a supervisory authority;
- Right to lodge a complaint with supervisory authority;
- Right to an effective judicial remedy against a controller or processor;
- Right to compensation.

4.4 The Trust shall maintain procedures, policies and notices to ensure that data subjects are informed about their rights.

4.5 Definitions

4.5.1 Personal Data
Personal data means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4.5.2 Special Category Personal Data
Special Category personal data is information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, physical or mental health or condition or sexual life or sexual orientation, genetic data and biometric data (for the purpose of uniquely identifying a natural person).

4.5.3 Data Subject
The data subject is a natural person identified or identifiable by personal data about whom we hold any personal data.

4.5.4 Processing
Processing means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.

4.5.5 Data Controller
The data controller is the natural or legal person, public authority, agency or other body or organisation which, alone or jointly with others determines the purposes and means of the processing of personal data.

4.5.6 Data Processor
The data processor is a natural or legal person, public authority, agency or other body or organisation that processes personal data on behalf of us as the data controller and on our instructions.

4.5.7 Recipient
A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

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

4.5.9 Data Protection Officer
The individual identified as having responsibility for the organisation's compliance with data protection law.

4.5.10 Data Protection Authority
This is the ICO as the body officially appointed by the UK to be responsible for monitoring and enforcement of the General Data Protection Regulation.

4.5.11 Subject Access Request
Any request made in writing by a Data Subject to have access to or be informed of the nature of personal data that the Trust holds about them.

4.5.12 Breach
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

4.6 Further definitions relating to data protection terminology can be found in appendix A.

5. Procedures

Fair and Transparent Processing of Data

5.1 Data Protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed fairly, data subjects must and will be made aware of the following in our privacy notices or requests to process data:

- That the personal data is being processed;
- Why the personal data is being processed;
- What the lawful basis is for that processing (see below);
- Whether the personal data will be shared, and if so with whom;
- The period for which the personal data will be held;
- The existence of the data subject's rights in relation to the processing of that personal data; and
- The right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

5.3 The Trust will only process data that is **necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any processing.**

5.4 Data collected for the purposes of public health (including visitor contact data for COVID-19) will be kept as long as required. Contact data for visitors will be kept for 21 days after the most recent visit, with information on visitors kept as per standard retention requirements. Public Health data may be shared with third-parties as required including, but not limited to:

- National Health Service (including NHS Test and Trace)
- Public Health England
- Other local health authorities

Data collected and processed for public health purposes is done so under GDPR Article 9(2)(i) which states: (in part) "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health..." and Recital 54 which includes: "The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject."

5.5 Collection and processing of visitor data will be documented in the privacy notices and in a statement available to visitors at the time of data collection to include the following information:

"We collect the following visitor information for the purposes of security, safety and public health:

- *Name*
- *Organisation*
- *Date and time of visit*
- *Contact details*
- *Car registration*

These are kept for six years in case of any claims by students, staff or visitors under the Limitations Act (1980). Should a positive test for COVID-19 be identified, relevant visitor data will be shared with the required public health authorities. Contact details will be deleted from any test and trace log after 21 days. For further details, please see the Data Protection Policy, or contact the Data Protection Officer."

Lawful Basis for the Processing of Personal Data

5.6 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection legislation. We will normally process personal data under the following legal grounds:

- The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a **legal obligation** to which the controller is subject (e.g. the Education Act 2011);
- Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
- Processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.

5.7 Special category data will not be processed unless a specific lawful basis as listed in Article 9 of the GDPR applies. When this special category data is being processed we will normally only do so under the following legal grounds:

- Where the processing is **necessary for employment law** purposes, for example in relation to sickness absence;
- Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- Where the processing is necessary for **health or social care purposes**, for example in relation to pupils with medical conditions or disabilities; and
- **Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.**

5.8 Full details of the categories of data subjects, the categories of personal data and the organisational and managerial measures used to secure this data are provided in the Trust's privacy notices.

Notification

5.9 As a public body the Trust is required to provide information to the ICO for inclusion onto the national data protection register. This notification contains the name of the data controller (the Trust), it's registered address, the name and contact details of the data protection officer and sets out the categories of personal data that we process, with whom we share the data and the reason for sharing.

5.10 The Trust is committed to transparency in its use of personal data. Appropriate privacy notices are provided to parents/carers when students join one of our schools and to staff when they are first employed. These notices set out:

- The Trust's legal basis for processing personal data, the types of data processed, the third parties that we share data with and the reason for sharing the data.
- The rights of the individual to access their personal data and how to make a subject access request.
- How to contact the ICO if they have a complaint.

5.11 Privacy notices are also accessible in the public areas and websites of all Trust schools.

Consent

5.12 When students, staff or our other members of our workforce join the Trust a consent form will be required to be completed in relation to them. Where appropriate third parties may also be required to complete a consent form.

5.13 In relation to all students under the age of 12 years old we will seek consent from an individual with parental responsibility for that student.

5.14 If consent is required for the processing of personal data of any data subject then the form of this consent must:

- Inform the data subject of exactly what we intend to do with their personal data;
- Require them to positively confirm that they consent (we cannot ask them to opt-out rather than opt-in); and
- Inform the data subject of how they can withdraw their consent.

5.15 Any **consent must be freely given**, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

5.16 The DPO must always be consulted in relation to any consent form before consent is obtained.

5.17 A record must always be kept of any consent, including how it was obtained and when.

5.18 There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include safeguarding, child protection and medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur. Please refer to the Trust Safeguarding and Child Protection Policy and Supporting Pupils with Medical Needs Policy for further information.

5.19 Further detail is included in the consent procedure (appendix 2).

Management of Personal Data

5.20 The Trust will ensure transparency and accountability in the way it collects personal data. All data subjects (usually staff or students/carers) will be provided with a privacy notice at the point in time their personal data is first collected as detailed in the data collection and records management procedure (see appendix 3).

5.21 To comply with data protection law all records containing personal data must have a defined lifecycle. During this period, there is an obligation to maintain the record and its accuracy. Document disposal dates are determined by the nature of the personal data, the Trust's other legal obligations and whether the processing purpose is still valid. See section 5.66 regarding retention policies.

5.22 The Trust will routinely carry out audits for each of its schools. These audits will assess areas such as data processing, storing and sharing. An example process for completing an information audit is described in the information audit procedure (see appendix 4).

Disclosure and Sharing of Personal Data

5.23 The Trust is committed to the strictest possible controls on the sharing of personal data with third parties.

5.24 All such arrangements must be approved by the Trust data protection officer and will be based on a clearly identified need that falls within the bounds of our processing statement. Shared data will be restricted to the minimum amount necessary to adequately meet the identified need and will only be transferred by a verified, secure method in accordance with the data sharing procedure (see appendix 5).

5.25 We may share personal data that we hold about data subjects with other organisations, without consent, where we have a lawful basis for doing so. Such organisations include the Department for Education and Education and Skills Funding Agency (ESFA), Ofsted, health authorities and professionals, the Local Authority, examination bodies, other organisations, and other organisations where we have a lawful basis for doing so.

5.26 The Trust will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence**.**

5.27 In some circumstances we will not share safeguarding information. Please refer to the Safeguarding and Child Protection Policy.

Security

5.28 The Trust will implement appropriate data security measures using policies, procedures and technologies to ensure and maintain the security of all personal data from the point of collection to the point of destruction.

5.29 These security measures will be appropriate to the risks in processing personal data and will be consistent with the rights of the data subjects.

5.30 These measures shall include as appropriate:

- Measures and data access controls to ensure that the personal data can only be accessed by authorised personnel for the purposes agreed in the record of processing activity and outlined in the organisation privacy notice;

- In assessing the appropriate level of security account shall be taken in particular of all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorised or unlawful storage, processing, access or disclosure of personal data;
- The anonymisation, pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regular testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing of personal data;
- Measures to identify vulnerabilities with respect to the processing of personal data in systems used to provide services to the Trust.

5.31 The Trust data security procedure (appendix 6) contains full details of the measures used to secure personal data including security for paper and electronic records and procedures for the workforce when working away from Trust premises. Security of paper-based information is further enhanced by the Trust clear desk procedure (appendix 7).

Data Protection Impact Assessments

5.32 The organisation takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

5.33 In certain circumstances the law requires us to carry out detailed assessments of proposed processing. This includes where we intend to use new technologies which might pose a high risk to the rights of data subjects because of the types of data we will be processing or the way that we intend to do so.

5.34 The Trust will complete an assessment of any such proposed processing and will use a template document which ensures that all relevant matters are considered. The procurement or implementation of a new process will only continue if the assessment indicates that privacy risks have been adequately addressed.

5.35 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

5.36 Further information on the data protection impact assessment procedure is included in appendix 8.

Data breaches

5.37 Where there is a personal data breach, the Trust will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

5.38 The procedure for data breaches, set out in appendix 9, will be followed.

Subject Access Requests

5.39 The Trust is committed to:

- Ensuring that individuals' rights to their own personal information can be appropriately exercised;
- Providing adequate training for staff to recognise and handle subject access requests;

- Ensuring that everyone handling personal information knows where to find further guidance on individuals' rights in relation to their own personal information;
- Ensuring that queries about individuals' rights to their own personal information are dealt with effectively and promptly;
- Being fair and transparent in dealing with a subject access request;
- Logging all subject access requests to assist the Information Commissioner's Office with any complaints related to subject access as well as identifying any issues that may assist in the identification of new data handling processes and training requirements.

5.40 All staff are responsible for ensuring that any request for information they receive is dealt with in line with the requirements of the GDPR and in compliance with this policy. All staff have a responsibility to recognise a request for information and ensure it is passed to the responsible member of staff and/or the DPO within two working days.

5.41 The subject access procedure (appendix 10) details all the necessary actions to be taken by the Trust.

Publication of information

5.42 The Trust maintains and publishes a publication scheme (or Freedom of Information scheme) on its website outlining classes of information that will be made routinely available, including policies and procedures.

5.43 Classes of information specified in the publication scheme will be made available quickly and easily on request.

5.44 The Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.

5.45 When uploading information to the organisation website, staff will be considerate of any metadata or deletions which could be accessed in documents and images on the site.

DBS data

5.46 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

5.47 Data provided by the DBS will never be duplicated.

5.48 Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

5.49 Data Subjects have the right to appeal against any automated decision making, such as a DBS check.

Photography, images and videos

5.50 Photographs and videos will only be collected and stored by the Trust with a documented lawful basis as in accordance with the consent procedure (appendix 2).

5.51 Photographs and videos will normally only be taken and used where they are deemed essential for performing the public task of the Trust or relative to providing education.

5.52 There may be occasions that arise where the Trust would like to celebrate the achievements of our students and therefore we may want to use images and videos of our students within promotional materials, or for publication in the media such as local, or even national, newspapers covering organisation events or achievements. If this is the case we will seek the consent of the students, and their parents where appropriate, before allowing the use of images or videos of students for such purposes.

5.53 Where photographs are required for other purposes, these purposes will be documented and explicit consent will be sought.

5.54 The retention period for photographs and videos taken by the Trust will be documented in the Trust retention schedule. At the end of the retention period photographs will either be destroyed or they may be retained as photos for archiving purposes in the public interest.

5.55 Parents and others attending Trust events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a Trust performance involving their child. The Trust does not prohibit this as a matter of policy.

5.56 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to control or prevent.

5.57 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

5.58 Whenever a student begins their attendance at the Trust they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that student. We will not use images or videos of students for any purpose where we do not have consent. An exemplar letter is included in appendix 2.

CCTV

5.59 CCTV may be used for the purpose of protecting the safety of staff, students and visitors and to help secure the physical premises. Please refer to the Trust's CCTV Policy.

5.60 Notices of recording including details of the Data Controller and where a copy of Trust CCTV policy can be obtained will be included on clearly visible signs posted at all entrances to the Trust sites.

5.61 All CCTV footage is securely stored and can only be accessed by appropriate members of staff. All images recorded by CCTV will be deleted as defined in the retention schedule.

5.62 Where the Trust installs new CCTV cameras, a data privacy impact assessment will be carried out prior to installation.

5.63 The nominated person responsible for CCTV in the Trust is the Special Projects Lead.

Retention schedule

5.64 The Trust will not keep personal data longer than necessary and will maintain a retention schedule outlining the retention requirements of electronic and paper records. The Trust will retain the minimum amount of information that it requires to carry out its statutory functions and the provision of services.

5.65 In circumstances where a retention period of a specific document has expired, checks will be made to confirm disposal and consideration given to the method of disposal to be used based on the data to be disposed of.

5.66 These checks will include the following questions being addressed:

- Have the documents been checked to ensure they are appropriate for destruction?
- Is retention required to fulfil statutory obligations or other regulatory obligations, including child protection?
- Is retention required for evidence?
- Is retention required to meet the operational needs of the service?
- Is retention required because the document or record is of historic interest, intrinsic value or required for organisational memory?

5.67 Retention data will be documented in the Information Record Management Society (IRMS) school toolkit (contact your Business Manager/Senior Administrator for more information).

Training

5.68 All Trust staff will receive either training or guidance to a minimum standard of understanding in data protection law appropriate to their role. This training and the assessment will be repeated annually and may be supplemented by additional training on the content of this policy and the associated procedures.

5.69 Additional face-to-face training will be provided to tackle specific matters relating to particular job roles and issues arising from subject access requests.

5.70 New staff will receive data protection training during their induction period rather than wait until the annual training occurs.

Enforcement

5.71 The Trust takes compliance with this policy very seriously as failure to comply puts staff, the Trust and potentially students at risk. The importance of this policy means that a failure to comply with any requirement including associated procedures may lead to disciplinary action and may result in dismissal.

Data Protection Procedures

5.72 The following procedures give detailed guidance in the areas described in this policy.

- Brooke Weston Trust Consent Management Procedure (appendix 2)
- Brooke Weston Trust Data Collection and Records Management Procedure (appendix 3)
- Brooke Weston Trust Information Audit Procedure (appendix 4)
- Brooke Weston Trust Data Sharing Procedure (appendix 5)
- Brooke Weston Trust Data Security Procedure (appendix 6)
- Brooke Weston Trust Clear Desk Procedure (appendix 7)
- Brooke Weston Trust Data Protection Impact Assessment Procedure (appendix 8)
- Brooke Weston Trust Breach Procedure (appendix 9)
- Brooke Weston Trust Subject Access Procedure (appendix 10)

6. Policy Review

6.1 This policy will be reviewed on a bi-annual basis or in response to changes in data protection legislation.

Document Control

Date of last review:	September 2021	**Author:**	Data Protection Officer
Date of next review:	September 2022	**Version:**	3
Approved by:	Strategic Delivery Group	**Status:**	Ratified

Summary of Changes

- Outline of Trust commitment as data controller ***(paragraph 1.2)*** and to proper and secure use of data in line with legislation ***(paragraph 1.3)***
- Outline of responsibility of Trust as data controller ***(paragraph 1.4)***
- Reference to ICO and DfE guidance regarding GDPR and data processing ***(paragraph 1.5)***
- Clarified policy applies to all staff and DPO as principal point of contact ***(paragraph 2.1-2.2)***

- Confirmed Strategic Delivery Group as body responsible for implementation of this policy ***(paragraph 3.2)***
- Outline of roles and responsibilities of the DPO and role of Trust in supporting them to fulfil their function ***(paragraph 3.3-3.9)***
- Inserted data protection principles ***(paragraph 4.2)***
- Inserted rights of data subjects which BWT will support ***(paragraph 4.3)***
- Updated definition of 'recipient' ***(paragraph 4.5.7)***. Further extended definitions are included in appendix A ***(paragraph 4.6)***
- Clarity on fair and transparent processing of data including reference to privacy notices setting out further information on how data is processed ***(paragraph 5.1-5.5)***
- Inserted grounds for processing of personal data ***(paragraph 5.6)***
- Section on 'consent' highlighted in main body of document rather than in appendix ***(paragraph 5.12-5.19)***
- Added under sharing of personal data, sharing data with other organisations where we have a lawful basis for doing so ***(paragraph 5.25-5.27)***
- Security information highlighted in main body of policy rather than in appendix ***(paragraph 5.28-5.31)***
- Data protection impact assessment summary information moved to main body of policy rather than in appendix ***(paragraph 5.32-5.36)***, as with data breaches ***(paragraph 5.37-5.38)*** and subject access requests ***(paragraph 5.39-5.41)***
- Added reference to publication of information (freedom of information) scheme ***(paragraph 5.42-5.45)***
- Added section on DBS data ***(paragraph 5.46-5.49)***
- Photography, images and videos highlighted in main body of policy rather than in appendix ***(paragraph 5.50-5.58)***
- Added section on CCTV ***(paragraph 5.59-5.63)***
- Reference to Information Record Management society school toolkit for retention schedule information ***(paragraph 5.67)***
- Training requirements for staff updated to annual training ***(paragraph 5.68)***

Appendix 1 – Definitions

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future;

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

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

Personal data breach means 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;

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

Supervisory authority means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR;

Cross-border processing means either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;

Relevant and reasoned objection means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

Information society service means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;

International organisation means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

Special categories of personal data means personal data:

- revealing racial or ethnic origin;

- revealing political opinions;
- revealing religious or philosophical beliefs or trade union membership;
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person;
- data concerning health or data concerning a natural person's sex life or sexual orientation;

Data breach: an incident or event in which personal and/or confidential data:

- has potentially been viewed or used by an individual unauthorised to do so;
- has had its integrity compromised;
- is lost or is unavailable for a significant period.

Appendix 2 – Brooke Weston Trust Consent Management Procedure

Overview

Trust schools seek consent (particularly from parents/carers) for a variety of reasons including school trips, use of student photographs etc. In most cases this consent will involve the processing of personal data (e.g. storage, sharing, transfer, printing). Where this is the case, the consent must be managed in compliance with data protection law.

This document explains the procedure that must be followed for the collection and management of consent from data subjects (students, parents and staff).

To comply with the high standard set by the data protection legislation we must ensure that:

- The consent is specific – the person giving consent is clear **what** they are being asked to consent to, **why** they are being asked and **what we will do** with any data related to the consent.
- We ask people to **positively opt in**, and without evidence of that opt-in we assume that we do not have consent.
- We make clear that they can withdraw their consent.
- We ensure that individuals can withdraw consent without detriment.
- We avoid making consent a pre-condition of a service we provide.

Scope

This procedure applies to all requests for consent that the Trust makes to students, parents or workforce.

Responsibilities

Trust Data Protection Officer

- Audit compliance with the consent procedure
- Audit maintenance of all consents
- Review of this procedure

School Principal

- Implementation of this procedure in the school

School Head of Administration/Data Manager

- Manage the collection of consents
- Manage consent withdrawals

Method

Consent Requests

As potentially every request for consent will be for a different circumstance it is not possible to be completely prescriptive in terms of method however where the request will involve the processing of personal information the request for consent **must** include the following:

1. Full details as to what the recipient is giving their consent for.

2. If we are sharing any personal information with a third party as a result of the consent it must detail;
   - exactly what information is being shared,
   - who the third party is that we are sharing the information with,
   - why the data is being shared
   - and what will happen to that information once the third party no longer needs to have it.

3. A means for the recipient to make a positive action to indicate consent e.g. a check box followed by a signature space (not a check box alone). (Ringing "Yes" or "No" is acceptable).

4. If the consent is not for a trip or single event i.e. the consent is for a series of events or for a continuous purpose like photographic use, it must include a statement that the consent can be withdrawn and instructions on how to do that.

Multiple Requests

If we are making multiple requests at the same time then each request must be clearly separated from the others with its own signature space that is clearly identified as related to that particular request.

Note:
In any circumstance where consent has been requested but we have *not* received a response we must assume that we *do not* have consent and act accordingly.

Data Management

The data protection legislation requires consent to be "actively managed" so having requested consent we need to be able at any point in time, to be absolutely sure that we still have the authority conveyed to us by that consent.

Local Management

To be sure we are still acting with consent it is critical to maintain accurate records and preserve evidence such as signed paper documents or electronic records where electronic forms have been used to gather consent e.g. sent via parental engagement app.

1. Where possible all consents should be recorded on the school Management Information System (MIS) to maintain it as the overall source for staff and student information.

2. Signed consent forms must be stored in the student or staff members paper record or if possible scanned and stored on the student or staff members record in the school MIS.

Management of Third Parties

Where personal information is shared with a third party (e.g. school trips) the Trust is still responsible for that personal data and its confidentiality. In order to maintain control of the data we must:

1. When making any booking, detail what personal data will be shared with the third-party organisation and why and obtain from them a written undertaking that they will securely dispose of the personal data shared with them once the purpose of the disclosure has expired i.e. the event or trip is over.

2. Follow up with the third party and obtain written confirmation that they have disposed of the data.

Managing Consent Withdrawal

We are required by law to inform those whose consent we have requested that they can withdraw it and we must provide a process that makes it "as easy to withdraw consent as it was to give it in the first place".
The authority conveyed upon us by consent holds only until that consent is withdrawn so we must maintain an up-to-date and timely record of any withdrawals. To assist with this all Trust schools should maintain a "consent@" email address accessible by appropriate staff.

1. Request forms for purposes which are not "one-off" (e.g. photograph permission) **must include the following standard instructions** on how to withdraw consent and include the "consent@" email address and the individual school's telephone number.

   ### Standard Wording:

   "The Trust understands that this is an active consent and you can withdraw your permission at any time. To do this contact the school by email on consent@<school email domain> or by phone on <school phone number> clearly stating which permission you are withdrawing."

2. On receipt of a withdrawal the MIS must be updated to this effect and any paper consent document marked as withdrawn, dated and signed by the staff member processing the withdrawal.

Review

This procedure will be reviewed in circumstances where a data protection breach has occurred as a direct result of a consent management issue, or in line with review of the Data Protection policy.

Example Request Wording

Example Request Wording
The request should match the following format:

1. Purpose – Why we are seeking permission? (Include as much detail as possible).
2. Scope – What are we sharing, where will it go, how long for? (Include as much detail as possible).
3. Rights related information e.g. deletion, amendment if any.
4. Standard consent statement.

For photographic and media permission:

"Student name:
Tutor Group (or Name of Primary School if joining in Year 7):
Date:

Dear <parent/carer name>,

<Insert school name> and the Brooke Weston Trust use photographs for identification, advertising and marketing purposes, and to celebrate achievement, including sharing photographs with local newspapers and putting them on social media (currently Facebook, Twitter and Instagram).

How we will use your child's image
Photographs used for marketing and advertising purposes will include use for adverts in newspapers, use in prospectuses and in newsletters and these may have a prolonged lifetime.

If a photograph is used to celebrate your child's achievements this will appear as a news article on the school's website and will be kept as an archived news article on the website indefinitely. If this photograph is shared with a local newspaper it could also be stored indefinitely by the newspaper in their archive.

Photographs used on social media could be stored indefinitely and could be redistributed outside of the control of the person or organisation that uploaded them. It may not be possible to retrieve or delete images posted on social media if your consent is withdrawn.

Less frequently video footage is used for promotional events such as open days/evenings, 6th Form open events and staff recruitment purposes. These materials may be archived (for reference purposes) indefinitely once the event is over.

You can request that archived photographs and articles be deleted at any time and we will be happy to oblige. For publications with a longer lifetime where a photograph is included we will ensure that it is not re-printed with that photograph if you request this.

<Insert school name> understands that this is an active consent and you can withdraw your permission at any time. To do this contact the school by email on consent@<school email domain> clearly stating which permission you are withdrawing or phone the school on <school phone number>.

Why are we asking for your consent?
You may be aware of the Data Protection Act 2018. To ensure we are meeting the requirements of this Act, we need to seek your consent to take and use photographs and video footage of your child. We really value using photos and video of students to be able to showcase what they do in school and show what life in our schools is like to others so we would appreciate you taking the time to give your consent again.

I am happy for photographs and video of my child to be taken and used for the purposes described above. ☐

I am NOT happy for the school to take and use photographs and video of my child. ☐

Parent or carer's signature:

Date:"

For a school trip permission:

"For your child to attend the <insert trip name/description> we are obliged, with your permission, to share information about your child with <insert third party provider's details>.

We will share <insert personal information e.g. name, DOB, allergies/medical conditions, emergency contact details> with them for safety/safeguarding reasons. Arrangements have been made with the provider to securely dispose of this information once the <trip/event> is over and their legal obligations have been discharged. The provider will send us written confirmation that this has occurred.

I give my permission for <parent inserts name of child> to attend the <insert trip name/description> on/between <insert date(s)>

Parent or carer's signature:

Date:"

Appendix 3 – Brooke Weston Trust Data Collection and Records Management Procedure

Overview

This document explains the procedures for data collection, storage, update, sharing, archiving and disposal, whether that data is held in paper or electronic form.

At all times, we must ensure:

- Personal data is secure
- That the data subject has been informed what we are processing, who we are sharing the data with and why it is being processed.
- It is being processed in line with our processing statement.
- The data is accurate and up-to-date.
- We know If the data processing is still necessary.

Scope

This procedure applies to all personal data processed by the Trust whether held electronically or on paper.

Definitions

Processing – any activity involving personal data including recording, storage, transfer and printing.

Personal Data – any information which alone or in conjunction with other information identifies a living individual.

Special Category Personal Data – personal data relating to medical conditions, sexual orientation, race or ethnic origin, trade union membership, religious beliefs, political opinions and biometric and genetic data.

Responsibilities

Trust Data Protection Officer (DPO)

- Review and maintenance of Privacy Notices
- Audit of records management
- Review of this procedure

School Principal

- Management of school staff engaged in processing personal data
- School implementation of this procedure
- Designation of the role of **Senior Administrator**

School IT Support

- Maintenance of electronic administration file structure and access rights
- Security of electronic administration files including backup
- Maintenance of the school Management Information System (MIS) and access rights
- Security of the school MIS

School Senior Administrator

- Maintenance of paper administration file structure and access rights
- Security of paper administration files
- Supervision of data entry onto the school MIS

- Management of paper records including storage, archiving and secure disposal

Administration Staff

- Collection of staff and student/carer personal data
- Processing of staff and student/carer personal data

Teaching Staff

- Management of paper and electronic teaching and assessment information

Method

Data Collection

Data collection usually occurs at specific points in the academic year i.e. when new students or staff join a school. Recorded personal data can be in both paper and electronic form, often occurring as an initial paper record which is then transferred onto the school management information system (MIS). The key processes of data collection are the same for either medium.

Collecting staff personal data – applications for employment

1. The administration staff **must** provide a link to the Trust Staff Privacy Notice at the point in the application process at which the personal data of the prospective employee is collected.

2. Completed applications from prospective staff **must** be secured at all times and access **must** be restricted to only those staff directly involved in the application process.

3. Once the application process is complete the successful candidate's information is transferred to the school MIS as soon as possible. Any information which is unclear should be verified with the new employee as soon as possible.

4. All applications from unsuccessful candidates **must** be disposed of **securely** once the successful candidate has formally accepted the position. No offer should be made to keep applications from unsuccessful candidates on file, bit candidates can choose to provide such information to the Trust via the "talent pool" database.

Collecting staff personal data in person

1. The administration staff provide the staff member with a copy of the Trust Staff Privacy Notice.

2. The administration staff explain the content of the privacy notice if face-to-face or offer further explanation if personal data is being collected remotely.

3. Any information collected that is not essential to the performance of the contract of employment, the job role or the wellbeing of the staff member (e.g. car registration number) will be subject to the employee's consent and should be collected only if a freely given and informed consent has been obtained. It must be made clear to the employee that there is **no obligation** to provide this information. This consent can be withdrawn at any time requiring the information collected under this consent to be erased. **Please refer to the Trust Consent Management Procedure** (appendix 2)**.**

4. The administration staff collect the required personal data and secure it as soon as possible. If possible, they should enter the collected data directly onto the school management information system (MIS).

Collecting student personal data – admission

1. The administration staff must include a copy of the appropriate Trust Student Privacy Notice in student admission packs.

2. Completed admission forms must be secured at all times and access must be restricted to only those staff directly involved in the admission process.

3. All consent obtained from parents/carers **must** comply with the Trust consent procedure (BWT-DPP02). The student or parents/carers **must** be informed that their consent can be withdrawn at any time by informing the school.

4. All information from successful applicants should be entered onto the school MIS as soon as possible. Any information which is unclear should be verified with the relevant parent/carer at the earliest possible opportunity.

5. Once the admission process is complete and all admission appeals have been heard all data obtained from unsuccessful applicants **must** be disposed of **securely**.

Collecting student personal data in person

1. The administration staff provide the student or their parents/carers with a copy of the relevant Trust Student/Carer Privacy Notice

2. If student is **at least** 12 years of age or over the administration staff explain the content of the privacy notice (if face-to-face) or offer further explanation if collecting pupil data from prospective parents.

3. All consent obtained from parents/carers must comply with the Trust consent procedure (BWT-DPP02). The student or parents/carers must be informed that their consent can be withdrawn at any time by informing the school.

4. The administration staff collect the required personal data and secure it immediately. If possible, they should enter the collected data directly onto the school management information system (MIS).

Storage of Personal Data

Personal data must be accessible only to those whose job role requires it. Brooke Weston Trust processes both ordinary and special category personal data in carrying out its responsibilities.

Paper Storage – Teaching and assessment materials containing personal data

1. School teaching staff **must** secure all teaching and assessment materials that contain personal data in locked filing cabinets when not in use.

Paper Storage – General materials containing personal data

1. School administration staff **must** secure all paper materials containing personal data in locked filing cabinets or secured areas.

Paper Storage – Significant files

1. Significant files are those paper files that contain either **significant quantities** of personal data (about one or more individuals) or **any special category data** including, but not limited to:
    a. SEN information
    b. Staff employment records
    c. Student education records
    d. Examination records, files and certificates

e. Financial records

2. The school administration staff **must** secure all **significant files** held on paper in an appropriate filing system in the designated locked filing storage.

3. The school administration staff **must** operate a check in/out system for all **significant files** (e.g. staff employment records or student paper records) using the form attached as Appendix 1. A copy of this check in/out form **must** be held in each filing cabinet. Authorised personnel removing a file indicate on the sheet which file they have removed and date and sign the form. When the file is returned the checking-in sheet is again updated and signed. All files containing personal data must be returned by the end of the working day.

4. All filing cabinets must be clearly labelled as to their contents and all keys must be appropriately marked to indicate which cabinet they are for.

5. The administration office must be equipped with a key cabinet that has a combination lock. When staff changes occur, the senior administrator changes the combination and informs the remaining staff of the change.

6. At the end of the working day the administration staff check that all files checked out have been returned and that all filing cabinets are locked and the keys to the cabinets are secured in the key storage box.

Electronic Storage – Teaching and assessment materials containing personal data

1. School teaching staff **must** secure all teaching and assessment files that contain personal data in the appropriate folder in the teaching file share.
2. Whenever a file is created that refers to a single individual the following file naming convention **must** be used:

   <AUTHOR>-<DATA SUBJECT ID>-<CONTENT DESCRIPTOR>-<DDMMYYYY>

   e.g. MRO-29131-Individual Learning Plan-05042018

   The Data Subject ID should be the roll/admission number, UPN or identifier that is used on the school Management Information System (MIS).

Electronic Storage – General materials containing personal data

1. School administration staff **must** secure all files containing personal data in the appropriate folder in the designated secure administration file share.
2. Whenever a file is created that refers to a single individual the following file naming convention **must** be used:

   <AUTHOR>-<DATA SUBJECT ID>-<CONTENT DESCRIPTOR>-<DDMMYYYY>

   e.g. MRO-Notes of Meeting-05042018

   If relevant, the Data Subject ID should be the roll/admission number, UPN or identifier that is used on the school Management Information System (MIS).

Electronic Storage – Significant files

1. The school administration staff **must** store all electronic personal data either on the school management information system (if appropriate) or in the appropriate folder in the designated secure administration file share.

Update of Personal Data

Personal data must be kept accurate and up to date out of responsibility to the data subject and our legal obligations as well as for the benefit of the school/Trust.

Day-to-day Changes

1. The integrity of records containing personal data **must** be maintained at all times. To enable this school administration staff must keep a log of changes received including an identifier for the individual whose data has changed, the date received, the date actioned and staff identifier for the person making the change. (The change log).
2. As soon as the school is made aware that personal information has changed the relevant records **must** be updated immediately. The school administration staff log the change and the date the notification of change was received without logging the exact data i.e. "John Smith address change".

Periodic Data Check

1. Once per academic year the administration staff produce a data checking sheet and distribute it to parents/carers. The data checking sheet must contain only the minimum data required to maintain the student records and must not contain any special category personal data e.g. data relating to health or SEN.
2. The letter to parents/carers sent out with the checking sheet must include a reminder that if their child has any specific medical needs or special educational needs and there has been any change in those needs that they should contact the school when they return the form.
3. As the number of forms returned is often low parents/carers should be reminded via the school and Trust websites, by social media and by any parental engagement applications to keep the school informed of any changes in their information, especially address and mobile phone numbers. These reminders should be issued on at least a quarterly basis.

Sharing

The sharing of personal data should only be carried out in accordance with the Trust Data Sharing Procedure (BWT-DPP08).

Retention and Archiving

The Trust has adopted the Information and Record Management Society's Toolkit for Schools as its standard for the retention and archiving of school records.

1. All personal data in either paper or electronic form must be retained and/or disposed of as dictated by the guidance in the IRMS toolkit.

2. When a student or staff member leaves all data on the school MIS that is not required to be retained according to the toolkit should be removed as soon as is reasonably practicable. This will be an ongoing process as each data item reaches its retention limit.

3. All data retained for statistical purposes e.g. examination or assessment results, Post 16 destination data, must be anonymised (student name substituted with a sequential number not related to the student's roll or admission number).

Disposal

Paper Records

1. Any personal information identified by the retention process as eligible for disposal must have its status verified by the senior administrator before disposal is carried out to ensure that the disposal is valid.

2. Personal information must be disposed by means of the schools confidential shredding service and a certificate of disposal must be obtained and stored as proof of compliance.

3. Disposal is recorded in the change log.

Electronic Records

1. Any personal information identified by the retention process as eligible for disposal must be have its status verified by the senior administrator before disposal is carried out.

2. The file and directory names of eligible personal information should be passed to the school IT Support team in order that they can be omitted from the backup regime.

3. The eligible files can then be deleted and the deletion recorded in the change log.

Review

This procedure should be reviewed as a result of any changes in storage systems (paper or electronic), changes to the school MIS or in line with review of the Data Protection policy.

Appendix 1: BWT Paper File Check In/Out Form

Brooke Weston Trust Paper File

Appendix 4 – Brooke Weston Trust Information Audit Procedure

Overview

All processing of personal data by the Trust and its schools must be accounted for. This is achieved by means of an information audit.

Scope

All Trust schools and the Trust central office.

Responsibilities

Trust Data Protection Officer (DPO)

- Review and monitoring of this procedure

School Principal

- Responsible for assigning the role of Senior administrator
- Ensuring that information audits are carried out
- Ensuring that new systems or methods of processing are included in the audit and where required a data protection impact assessment is carried out.

School IT Support Team and School Senior Administrator

- Work together to conduct information audits on systems processing personal data

Method

Initial Information Register

1. The responsible staff **must** create a register of information flows into and out of the school (or central office). All sources of personal data coming into or being transferred out of electronic or paper systems must be recorded in the BWT Data Processing Register (attached as Appendix 1). It may help to draw a diagram of data flows into and out of the school as a first step.
2. The register **must** be filled in with the school name (or central office), date of creation/modification and the names of the staff conducting the initial audit.
3. Inward and outward flows **must** be recorded on the relevant tab of the register including the data item, the source and destination of the data, the method of data transfer and the location of the destination system. More information can be added to the notes column of the register to clarify the information flow or process.
4. Once the register has been created a copy **must** be sent to the DPO so that it can be reviewed to identify processes or transfers that require a data protection impact assessment. These will be recorded in the register.
5. Where necessary the DPO will carry out a data protection impact assessment according to the BWT Data Protection Impact Assessment Procedure (appendix 8) and record the reference for the assessment in the register against the process/information flow concerned.
6. If the outcome of the impact assessment is of concern the DPO will act in accordance with procedure and may suspend the processing operation.

Updates to the Register

1. Once the initial register is complete it **must** be updated whenever a new information flow/process is introduced.
2. In this case the data protection impact assessment will have already taken place to authorise the new information flow/process and the reference for the assessment **must** be entered into the register.

Review

This procedure should be reviewed as a result of any changes in data protection legislation, or in line with review of the Data Protection policy.

Appendix 1 BWT Data Processing Register

Appendix 5 – Brooke Weston Trust Data Sharing Procedure (BWT-DPP08)

Overview

The sharing and transfer of personal data presents a potential risk to the rights of data subjects and therefore:

i. It should not be undertaken unless absolutely necessary
ii. It should only be undertaken by approved methods
iii. Only the minimum data required must be shared or transferred

Scope

All personal data that is shared whether internally or with external parties.

Responsibilities

Trust Data Protection Officer (DPO)

- Review and monitoring of this procedure

School Principal

- Responsible for assigning the role of Senior Administrator
- Enforce good data sharing practice

School IT Support team and School Senior Administrator

- Monitor data sharing arrangements and report issues and procedure violations

Method

1. **General Principles**

   Before any personal data is transferred the following checklist **must** be considered:

   a. Is the data sharing/transfer absolutely necessary? If not then no sharing/transfer should be made.
   b. Is the recipient authorised to receive/view the data being transferred? If not the sharing or transfer should be deferred until an appropriate recipient can be identified.
   c. Is the data to be transferred the minimum required for the purpose? If not, then the data should be reformatted to include only the necessary data types/items.

2. **Sharing/Transfer**

   Assuming that the answer to all of the above questions is yes, the following methods should be used for the transfer of the personal data depending on the type of sharing/transfer. **Where options are given, in all cases the first option listed is the preferred option and should be the option used if possible.**

   2.1 Internal Transfer

   When personal information needs to be shared with more than one staff member at a time within the same school:

   Electronic Sharing/Transfer

   Option 1. – The personal data files are placed in an **appropriate** administration file share and their location is communicated to staff via email.

   Option 2. – The personal data is shared by means of an encrypted memory stick or USB drive that has a complex password (minimum of 8 characters in length, at least one capital letter, at least one symbol and at least one number). **N.B this method will result in copies of the data which must be appropriately secured and managed so it should only be used as a last resort.**

Paper Sharing/Transfer
Internally, personal information should be shared by means of individually numbered copies of the information assigned to specific staff members and recorded in a list by the issuer. The issuer is responsible for recovering all copies of the data and disposing of them appropriately.

2.2 External Transfer
When personal data needs to be shared with an external third party:

Electronic Sharing/Transfer
Option 1. – The sharing/transfer is achieved by means of the approved and impact assessed transfer method provided by the recipient. The IT support team can advise on the appropriate method.

Option 2. – The sharing/transfer is achieved by means of an encrypted email service e.g. Egress

Paper Sharing/Transfer
Option 1. – Delivery by hand to the intended recipient.

Option 2. - The only other viable option for sharing personal data in paper format with an external third party is by Royal Mail Special delivery or by means of a courier service that offers a "track and trace" service, where a recipient signature is recorded and:

a. The personal data is packaged robustly to avoid damage in transit
b. The package is addressed to an appropriate named individual at the external third party
c. The package is clearly marked "Private and Confidential"
d. The sender name and address are recorded on the package to allow it to be returned if it cannot be delivered

2.3 School-to-School Transfer (between Trust schools)
When personal data needs to be shared between Trust schools:

Electronic Sharing/Transfer
Option 1. – The personal data files are uploaded to one of the Trust's online file sharing and collaboration services (Box or Microsoft OneDrive) and shared with the intended recipients. An appropriate access expiry date **must** be set (based on how long access to the information is required) and access must be set appropriately e.g. to read-only not download.

Option 2. – The sharing/transfer is achieved by means of an encrypted email service e.g. Egress

Option 3. – The personal data is shared by means of an encrypted memory stick or USB drive that has a complex password (minimum of 8 characters in length, at least one capital letter, at least one symbol and at least one number). **N.B this method will result in copies of the data which must be appropriately secured and managed so it should only be used as a last resort.**

Paper Sharing/Transfer
The only viable option in this case is by hand delivery to the intended recipient.

Review

This procedure should be reviewed as a result of any changes in data protection legislation, or in line with review of the Data Protection policy.

Appendix 6 – Brooke Weston Trust Data Security Procedure

Overview

The security of both paper and electronic records and IT services that process personal data underpins our compliance with the General Data Protection Regulation.

Security is founded on the three principles of Confidentiality, Integrity and Availability and these apply whether the systems are based on paper or are electronic.

Confidentiality – are systems protected from unauthorised access?

Integrity – is data protected from deletion or alteration unless by authorised personnel?

Availability – is there timely and uninterrupted access to systems and data?

This procedure addresses measures that must be followed for both paper and electronic systems to ensure our compliance with the above principles and therefore with the GDPR.

Scope

This procedure covers all paper and electronic systems that hold data but in particular those systems that process personal data (e.g. hold, store, transfer etc.) and/or whose availability affects the Trust's ability to meet its obligations to data subjects (staff, students and parents).

Responsibilities

Trust Data Protection Officer (DPO)

- Review and monitoring of this procedure

Special Projects Lead

- Work with the IT team to produce a disaster recovery/business continuity plan.
- Review of the Trust Data Security Procedure

School IT Support

- User account management
- Management of access rights on all electronic file storage
- Creation of a backup plan that meets the general standards laid down in this procedure
- Management of electronic backup systems
- Management of IT systems
- Flagging where systems or processes are inadequate to meet the requirements of this procedure

School Senior Administrator

- Maintenance of paper administration file structure and access rights
- Security of paper administration files
- Supervision of data entry onto the school MIS
- Management of paper records including storage, archiving and secure disposal

School Administration Staff

- Maintain the check in and out process for paper files

Method

Paper Records and Storage

Security for paper records mainly revolves around physical access and checking validity of changes or deletions.

Confidentiality

1. All paper files containing personal data **must** be secured from unauthorised access this is best achieved by keeping them physically separated from other files in an administration office or area out of general circulation.
2. Files **must** be secured in locked filing cabinets, clearly labelled with the nature of their contents. Cabinet keys must be labelled to identify which cabinet they belong to.
3. All keys **must** be secured in a combination safe inside the administration office. The combination must only be divulged to staff who have direct responsibility for the files.
4. If a member of administration staff leaves, the senior administrator will change the combination to the key safe and inform the relevant staff of the new combination.

Integrity

Update of Records

1. The integrity of records containing personal data must be maintained at all times. To enable this, school administration staff **must** verify that that any changes requested to personal data are **valid** before logging and actioning the change (as per the data collection and records management procedure (BWT-DPP04)
2. As electronic systems are more easily maintained than paper records, all personal data held on paper are considered to be originating documents and the electronic records held in files or on the school Management Information System (MIS) are considered to be the definitive record where there are discrepancies.

Priority must therefore be given to maintenance and update of electronic records and the update of paper files should be considered only where there is no matching electronic record.

Disposal of Records and Data

1. When a record requires deletion (as a result of a valid request to cease processing or because the record has reached its retention limit) the deletion **must** be approved by the senior administrator as per the data collection and records management procedure (BWT-DPP04) to avoid accidental deletion.

Availability

1. The whereabouts of all paper records containing personal data must be known at all times. All paper records containing either significant amounts of personal data or special category personal data **must** be checked in and out of filing cabinets using the check -in/out sheets as per the data collection and records management procedure (BWT-DPP04).

IT Systems

Confidentiality

Security for electronic files is highly dependent on good management of user accounts, passwords and files and file share permissions.

Physical Security

1. The IT Support team r and IT support staff **must** ensure that all IT hardware including network switches, firewall devices, Internet filters, servers, printers and client devices have an access password set to prevent unauthorised setting changes being made or additional hardware components added.

2. The IT Support team **must** ensure that all physical infrastructure assets are secured in locked cabinets or inside locked comms/server rooms. The keys to all cabinets and rooms will be clearly labelled and secured in a combination safe in the IT support office.
3. The IT Support team (or designated staff in their absence) is responsible for ensuring that cabinet keys are secured in the safe at the end of each day.
4. When a member of the IT support team resigns, the IT Support team will change the key safe combination and inform the relevant staff of the change.

User Accounts

1. All users of IT systems **must** be assigned a named user account which is unique to them. This account is provided on the basis that the user agrees to abide by the Trust Acceptable Use Policy.
2. The senior administrator **must** inform the IT Support team when it is known that a member of staff who has been issued with a user account is leaving Trust employment. The IT Support team then assigns an end date to the user account so that access to IT systems is unavailable at the point that the staff member leaves.
3. The account password **must** conform to the following complexity standard:

a. The password must be a minimum of 8 characters long
b. It must include at least one upper case letter
c. It must contain at least one lower case character
d. It must contain at least one number

4. The IT Support team must enforce password expiry such that password changes are enforced at least every 90 days and enforce password history restrictions such that every user must have at least three unique passwords before an old password can be reused.
5. For certain key systems and key user roles such as administrators, two means of authentication will be used wherever possible.

File Security

1. The IT Support team will ensure all electronic file storage is divided into separate areas corresponding to job roles and levels of responsibility. These areas will be assigned to users by means of separate file shares.
2. Personal data will be stored in labelled directories in a confidential area and this confidential area will be assigned as a separate file share with restricted permissions only to those staff with responsibilities for that data.
3. Within the file shares the IT Support team will assign specific file access rights to each directory to further restrict access to only the appropriate users.
4. Where possible the IT Support team will enable file logging on confidential folders and shares and monitor the access logs on a regular basis.

Integrity

The integrity of IT systems depends on services like a clean power supply, cooling/ventilation, a correctly planned, configured and tested backup solution and timely software updates.

Power, cooling and ventilation

1. The IT Support team and IT support staff will ensure that all IT systems have an adequate and clean power supply. A clean supply will be achieved by means of surge protection or the use of an uninterruptable power supply (UPS) unit which is capable of surge protection.
2. Wherever possible the IT Support team will ensure that key systems are supported by a UPS unit adequate to provide at least 15mins of power support to those systems and configured to automatically shut down the dependent systems before the battery expires.
3. The IT Support team will ensure that cooling systems are operational and regularly serviced such that infrastructure assets remain within their operational temperature tolerances.

Backup

1. The IT support team will create and operate a backup plan that meets the following general guidelines:
   a. The backup plan identifies data and applications requiring backup and ranks them by criticality with appropriate Recovery Point and Recovery Time objectives (RPO and RTO)
   b. The backup plan makes use of the fastest backup media possible
   c. If possible, the plan incorporates the use of intermediate disk backup i.e. disk-to-disk-to-tape
   d. backups are performed out of hours wherever appropriate
   e. data that changes daily is backed up daily
   f. where possible shared folders are configured to use shadow copy as a supplement to the backup plan
   g. there is a full backup of all data at least once a week
2. The backup plan must include arrangements for the transfer of backup media to the Trust's offsite storage at appropriate intervals.
3. Cloud backup should be used as the final destination for data in the backup plan (rather than tape) wherever possible.
4. The IT support team must ensure that backup jobs are monitored and any errors are addressed as soon as possible.
5. The IT support team must ensure that recovery capability is tested on at least monthly intervals by recovering a random selection of files from across the monthly backup set. These tests should be logged along with any actions arising from the test results.

Availability

The availability of IT services depends on where the service resides/is supplied from, the availability of resource and the quality and readiness of disaster recovery/business continuity plans. Software updates are an unavoidable part of operating IT systems and so need careful management to avoid impact on end-users.

Strategy

1. The IT support team will create appropriate disaster recovery plans for each school identifying prioritised key services and their recovery arrangements.
2. The IT support team r will seek to make use of Cloud services where there are clear advantages in terms of accessibility, availability, reliability and support over locally hosted applications or services (subject to satisfactory data protection impact assessments).
3. To facilitate the availability of Cloud services the Trust will procure and maintain appropriate Internet connectivity. Where possible the connectivity arrangements will include a minimum level of backup connectivity to allow access to critical services if the main connection is unavailable.
4. Where services or applications are provided locally, the IT support team will seek to host these services on virtualised hardware appropriately configured to provide spare resource and automated failover.

Monitoring

1. The IT support team will regularly monitor local server and application event logs to ensure errors and warnings are swiftly addressed and school staff are alerted to any issues.
2. The IT support team will regularly monitor the status pages of any Cloud applications to respond to service degradation issues and to ensure planned service outages are impact assessed and any potential effect is communicated to school staff.
3. The IT support team will ensure that where appropriate, infrastructure assets are configured to raise automatic email alerts when hardware issues arise and will ensure all infrastructure assets are regularly monitored for alert conditions.

Patching and Updates

1. The IT support team will maintain all applications and services at the highest possible level of update.
2. All patches or updates identified as critical by software manufacturers will be applied in a timely manner (once risk assessed) by the IT support team.

3. The IT support team will design and operate a software update/patching schedule in line with industry best practice and manufacturer release timetables.
4. Where possible updates and patches will be applied outside of normal working hours or in vacation periods. Where this is not possible the IT support team will ensure that school staff are made aware of any availability issues and that these are planned to avoid critical school activities e.g. exam result release dates.
5. The IT support team will ensure that firmware updates are performed in a timely manner (i.e. after appropriate risk assessment) on all infrastructure assets.

Antivirus and anti-malware

Virus and Malware attacks have a potential impact on the confidentiality, integrity and availability of IT systems. Effective antivirus and anti-malware protection is essential to mitigate these risks.

1. The IT support team will ensure that where appropriate, client devices and server equipment is protected by antivirus software.
2. This software must be capable of automatically updating itself and forcing an update if the end-user refuses update requests.
3. The IT support team **must** ensure that the update status of any client or server can be easily established and is regularly monitored.
4. Mobile client devices **must** be able to receive antivirus updates when not within the school network e.g. on home broadband connections.

Review

This procedure should be reviewed as a result of any changes in IT systems or paper storage systems, or in line with review of the Data Protection policy.

Appendix 7 – Brooke Weston Trust Clear Desk Procedure

Overview

A clear desk procedure is an important tool to prevent unauthorised access to confidential and personal data in staff work areas. The procedure also serves an important role in raising staff awareness of the need to protect sensitive and personal data.

Scope

All confidential, sensitive or personal data and electronic information resources in staff work areas.

Responsibilities

Trust Data Protection Officer (DPO)

- Review and monitoring of this procedure

All Trust Staff

- Awareness and compliance with the procedure

Method

1. All Trust staff **must** ensure that all confidential or personal information in electronic or paper form is secure in their work area at the end of the day and when they are away for more than a short period.
2. Desktop and laptop computers **must** be locked or shutdown when the work area is unoccupied.
3. Any personal or confidential information **must** be removed from the desk and locked in a draw when the desk is unoccupied and at the end of the working day.
4. Filing cabinets containing confidential or personal data **must** be kept closed and locked when not in use or when not attended.
5. Keys for filing cabinets **must** be secured at all times.
6. Laptops and portable storage devices **must** be locked with a locking cable or locked away in a draw if they are being left in the work area.
7. **No** passwords are to be written down and stored anywhere in staff work areas.
8. All whiteboards containing confidential or personal data **must** be erased.
9. Printouts containing confidential or personal data **must** be removed from the printer immediately.

Review

This procedure should be reviewed as a result of any changes in data protection legislation, or in line with review of the Data Protection policy.

Appendix 8 – Brooke Weston Trust Data Protection Impact Assessment Procedure

Overview

Any processing of personal data that represents a high risk either in terms of the amount of data being processed or the sensitivity of that data (or both) must not be undertaken unless an assessment of the risks to the rights of data subjects has been carried out first.

If any new processing or change to processing is to be accomplished by means of new technologies then this necessitates a risk assessment regardless of the sensitivity or volume of personal data involved.

This risk assessment is known as a Data Protection Impact Assessment (DPIA) and must be formally recorded and stored as part of the Trust's compliance documentation for data protection.

A form for completing a DPIA is attached as Appendix 1.

Scope

All processing activity that includes high volumes of personal data and/or special category personal data and any processing activity that relies on an IT system, particularly those systems hosted in the Cloud.

Definitions

Processing – any activity involving personal data including recording, storage, transfer and printing.

Personal Data – any information which alone or in conjunction with other information identifies a living individual.

Special Category Personal Data – personal data relating to medical conditions, sexual orientation, race or ethnic origin, trade union membership, religious beliefs, political opinions and biometric and genetic data.

Data Controller ("Controller") - the entity that decides on the nature of the data processing and the data subjects whose personal data is to be processed.

Data Processor ("Processor") - any entity that processes personal data on behalf of a data controller.

Responsibilities

Trust Data Protection Officer (DPO)

- Review and monitoring of this procedure
- Review and approval of all data protection risk assessments

School IT Support

- Conduct data protection impact assessments on school IT-based systems

School Senior Administrator

- Conduct data protection impact assessments on school paper-based systems

Method

The following general procedure must be followed to conduct an **adequate** data protection impact assessment. Some sections of the assessment will require evidence to be collected to back up the school/Trust's compliance with legislation e.g. from a third-party data processor.

More complex systems or those where either significant quantities of personal data or special category personal data is processed, will require more detailed evidence of assessment and supporting evidence of any third-party compliance with the legislation.

The method below is designed to assist in filling in the Data Protection Impact Assessment form attached as Appendix 1.

1. **Description of Processing**
   The first part of the assessment must provide a systematic and detailed description of the data processing.
   a. The nature and scope of the processing **must** be recorded e.g. a paper system encompassing all student data and data will be retained for a year (*what, who and how long*).
   b. The types of personal data being processed **must** be recorded in detail.
   c. A functional description of the processing operation **must** be recorded.
   d. All assets on which the personal data rely **must** be recorded e.g. hardware, software, networks, people, paper and paper transmission channels.
   e. Record should be made of any ICO codes of practice that are applicable and a description of how the processing meets those codes e.g. ICO CCTV Code of Practice.

2. **Necessity and Proportionality**
   The impact assessment needs to address the necessity of processing (if we don't need to do it, we shouldn't) and if it is necessary, then we need to consider if it is proportionate in terms of whether the data processed is sufficient and relevant to the purpose and also limited to only that data required for the purpose (i.e. we are not processing data that we don't need to to meet the stated purpose). We must also have a schedule in place to determine when the data is disposed of and state how we are going to comply with the specific rights of data subjects.

   a. The impact assessment **must** record the specified, explicit and legitimate purpose of the data processing and **must** indicate that no expansion of the processing will take place that goes beyond the legitimate purpose.
   b. The assessment **must** address the lawfulness of the processing. The most likely lawful purposes being:
      i. The performance of a contract to which the school or Trust is subject e.g. if the Trust were to set up a pupil referral unit operated under contract to a local authority.
      ii. A legal obligation to which the school or Trust is subject e.g. our obligation to provide an education to our students under the Education Act.
      iii. Our legitimate interests (school or Trust) e.g. providing cashless catering services to students. (Processing that is of benefit to staff, students and/or their parents/carers).
      iv. The consent of the data subject(s). This is an absolute last resort. Consent should **only** be used when there is no other basis on which to process with the full understanding that the consent can be withdrawn at any time and that we are responsible for providing the means for the data subject to manage their consent.
   c. The assessment must address whether the personal data being processed are **adequate**, **relevant** and **limited** only to the stated processing purpose i.e. we are not storing or using data as an additional benefit of having collected it when it does not serve the original purpose.
   d. The duration of data processing **must** also be addressed in the impact assessment. As much detail as possible is required, so if the processing is storage for example, we must detail how long we expect to store the personal data and on what basis we will cease storage e.g. when a student leaves the school.
   e. The assessment must include the measures we are taking to preserve the rights of data subjects in answer to the following questions:
      i. What information is provided to the data subject about the processing? *Here we would normally refer to the privacy notices posted on the Trust website and indicate that data subjects are pointed to them.* **N.B. those conducting the risk assessment must inform the DPO of the new processing so that the relevant notice can be updated (subject to a satisfactory risk assessment).**

ii. What is our procedure that supports the data subject's right of access? *Here we would normally refer to the Trust Subject Access Procedure (BWT-DPP06) unless the system concerned provides a different means of dealing with data subject access.*
iii. What procedure do we have in place to address the data subject's right of rectification and erasure? *Here we would normally refer to the Trust Data Collection and Records Management Procedure (BWT-DPP04).*
iv. How do we address the data subject's right to object to processing of their personal data? *If our processing is based on our obligations under an act of Parliament (e.g. The Education Act) then this will supersede the right of objection. In this way a student cannot request that we stop maintaining their record on our MIS system as we are obliged to in law in order to keep account of their education, contact their parents and look after their vital interests.*
v. Where we are using a processor, how are we formalising that relationship? *Here we need to mention that we will have a **contract** in place with the processor and this will include the details of the processing in terms of data subjects, data types, the scope of processing, the fact that we are the controller and they must act in accordance with our written instructions, that they must not use a sub-processor (subcontract) without our express written permission and that they have sufficient technical and organisational measures in place to safeguard personal data.*
vi. If we are making use of a processor, where geographically is our data held and what guarantees are there that this situation will remain the same? *Here we need to establish that data will be held in EU or UK based datacentres, that this is guaranteed by the processor and that they will contact us if they plan to change this?*

3. Risks to rights and freedoms of data subjects

In this section of the assessment the risks to data subjects must be identified and quantified in terms of likelihood of occurrence, severity and their impact on the data subject and their rights.

a. The assessment must identify the threats relating to illegitimate access, undesired modification and data loss and their sources.
b. Potential impacts to data subject's rights and freedoms **must** be assessed and their severity quantified.
c. Measures to eliminate or reduce the risks must be recorded with associated evidence e.g. if a processor says they meet the ISO 27001 information security standard, that should be recorded along with a copy of the compliance certificate.
d. It is critical that we take nothing provided by a third party at face value. Any claims or assertions relating to processing carried out on our behalf **must** backed by evidence that fully supports the claim. If this cannot be provided then the assessment **must** include measures the school/Trust has taken to independently verify such claims and any supporting evidence.
e. In addition to a description of the risks they must be summarised in the risk register section of the assessment form with their likelihood (low, medium, high), impact (low, medium, high) and mitigations.
f. A final decision on the overall risk must be taken in order to assess whether the planned processing can be undertaken. No risk of high likelihood and high impact can be tolerated and the conclusion of such an assessment would be that the processing activity could not be entered into.

4. Stakeholder Involvement

a. Where appropriate the views of data subjects can be surveyed and included in the impact assessment. This is **not** consent but is evidence that data subjects were consulted and saw the processing as either acceptable or of benefit to them.
b. The advice of the Information Commissioner's Office (ICO) can be sought where there are unmitigated high risks in the processing but it is seen as critical to the school/Trust's operations.

Review

This procedure should be reviewed as a result of any changes in data protection legislation, or in line with review of the Data Protection policy.

Appendix 1: BWT Data Protection Impact Assessment Form

Appendix 9 – Brooke Weston Trust Data Protection Breach Procedure

Overview

This document explains the procedure that must be followed in the event of a data protection breach.

A data protection breach has occurred if any of the following is true:

- Personal information has been lost or misplaced.
- Personal information in either electronic or paper form has been shared with an unauthorised third party accidentally or maliciously. This could be by email, telephone, post, file transfer or just handed out.
- There has been unauthorised access to personal information in either electronic or paper form. This could be by hacking/phishing activity, physical break-in or by the malicious activity of an insider to the organisation.
- The password of any account that can access a computer system holding personal data, has been disclosed. This can be accidentally or maliciously.
- A Trust-issued mobile device (mobile phone, tablet or laptop) has been lost or misplaced, even if the device is encrypted or PIN protected.
- An error in personal information held about a student, parent or staff member has had some form of impact on that person e.g. incorrect attendance data for a student has led to a fine being imposed on their parents.
- A system or service is unavailable and this has had an impact on one or more individuals whose personal data we hold e.g. The safeguarding system is unavailable meaning an incident affecting as student is not recorded and relevant safeguarding staff are not alerted.

Scope

This procedure applies to all personal data processed by the Trust whether held electronically or on paper.

Responsibilities

Trust Data Protection Officer (DPO)

- Assembly of the Data Protection Board
- Coordination of all remedial activity
- Reporting to the Information Commissioner's Office

School Principal

- Alerting the DPO of a data breach as soon as it is identified
- Reporting to the affected data subjects
- Management of school staff engaged in remedial activity
- Designation of the role of **Senior Administrator**

School IT Support

- Coordination of any investigative, remedial or supporting activity relating to IT systems

School Senior Administrator

- Coordination of any investigative, remedial or supporting activity relating to paper-based systems

All Trust Staff

- Reporting any suspected data breach to the school Principal

Method

1. **Log -** The Trust Data Protection Officer opens a breach log including the details known, the person or entity reporting the breach, the date and the time. This date and time signify the start of a 72-hour clock within which the Information Commissioner's Office must be informed if a breach has occurred.
2. **Assemble -** The DPO assembles the Data Protection Board from the staff in the responsibilities section above, or their substitutes.
3. **Verify -** The details of the breach log are examined by the Board to confirm:
   a. That personal data has been disclosed, or
   b. That there is doubt whether personal data has been disclosed, or
   c. It is clear that no personal data has been disclosed in which case "no breach" is recorded in the log, the time and date are recorded and the log is closed.
4. **Identify –** The Board identifies who is affected, what type of data has been disclosed, how much data if any, has been disclosed and the circumstances of the breach? The DPO enters these into the log.
5. **First Response –** The School IT Support team and/or School Senior Administrator carry out any immediate actions that will contain the breach or prevent further disclosure. The DPO enters details of these actions into the log.
6. **Inform –** The School Senior Administrator contacts those data subjects who are affected. The communication is made up of the following elements:
   a. An apology for the disclosure
   b. Full information on what has been disclosed
   c. Advice to the data subject as to how they can protect themselves from any consequences of the disclosure e.g. identity theft
7. **Notify –** The DPO informs the Information Commissioner's Office of the breach as soon as possible after the data subjects have been informed and in any case within 72 hours of the time and date entered into the log in Step 1.
8. **Further Action –** The Board carry out any further actions required to recover or dispose of the disclosed data/contain the breach, or as directed by the assigned ICO case officer.
9. **Update Data Subjects –** The Senior Administrator updates data subjects on the status of the breach – repeated regularly until the breach is closed.
10. **Update ICO –** The DPO updates the ICO on the status of the breach – repeated regularly until the breach is closed.
11. **Lessons –** Once the breach is closed the Board finalise the cause of the breach and identify preventative measures. If necessary the DPO arranges further/enhanced training for staff. The DPO records these actions in the log.
12. **Close –** The Board formally close the breach log.
13. **Report –** The DPO submits a report at the next available Operations Group meeting and submits the breach log to form part of the minutes of that meeting.

Review

This procedure will be reviewed and if necessary amended after any data protection breach, or in line with review of the Data Protection policy.

Appendix 10 – Brooke Weston Trust Subject Access Procedure

Overview

The individuals whose personal data we process (e.g. store, record, print etc.) have a right to see that information and be provided with electronic and/or paper copies of it. This is known as a **Subject Access Request** (the individual is known as the **Data Subject**).

Requests for access could be for very specific information or could be for everything that we hold about the individual.

Note:
The time limit for response to a subject access request is one month from receipt of the request.

Scope

All personal data processed by the Trust whether held electronically (files) or on paper.

Responsibilities

All Staff and School Governors

- Recognition of requests and prompt forwarding of them to the Trust DPO

Trust Data Protection Officer (DPO)

- Log subject access requests
- Monitor and advise on response to access requests
- Liaison with the Information Commissioner's Office where necessary

IT Support Team

- Coordination of support activity relating to access requests e.g. assisting with the location/recovery of electronic files

School Senior Administrator

- Coordinate the collation of subject data
- Supervise the verification of data subject identity
- Formal response to subject access requests

School Administration Staff

- Verification of the identity of data subjects
- Assisting in the collation of subject data

Method

1. **Identify** – In order to be valid, Subject Access Requests (SARs) must be made in writing (electronic or paper) by the data subject or a third party they have authorised to act on their behalf. SARs do **not** have to mention the General Data Protection Regulation or make any mention of data protection law to be valid, they simply have to request personal information about the individual concerned.

   The request can be sent to anyone associated with the school or Trust so all staff will be trained in recognising subject access requests and in this procedure.

2. **Inform** – Any member of staff receiving a subject access request **must** forward it to the DPO immediately. If received in letter form the request should be scanned and emailed to the DPO.

   On receipt of the request the DPO will log receipt, recording the time and date of receipt. The DPO will then ask the school administration staff to contact the data subject to formally acknowledge receipt of the subject access request.

3. **Verify** – Before a response can be made the school administration staff must verify the identity of the requestor. For example, If the request is in the form of a letter from the data subject, then the address on the letter can be cross checked with student or staff records. A second form of verification should be made by asking the requestor for certain pieces of information held on record (at least two) e.g. date of birth and mobile phone number.

   Student requests
   Students are considered to be legally competent to exercise their subject access rights if they are able to understand in broad terms what it means to make a subject access request and how to interpret the information they receive as a result of doing so. A reasonable approach is to assume that children who are at least 12 years of age are legally competent unless the school has good reason to believe otherwise.

   There may be situations where the nature of the material requested means that the school would have reservations about releasing it to the student. In these situations, advice **must** be sought from the Trust's legal advice provider.

   Requests made by third parties
   If the request is made through a third party then contact should be made with the data subject concerned by means of contact details held on record in order to confirm that they have engaged the third party to act on their behalf.

   If the request is made by a student's parent or carer on behalf of the student and that student is at least 12 years of age (i.e. at least Year 8) then their authorisation **must** be obtained before any information can be released.

   Once the data subject's identity is verified the DPO **must** be informed immediately that the request is valid.

4. **Refine** – If the request is very general e.g. "everything you hold about me" the data to be collated will be very large. The school administration staff should contact the data subject in writing and request that they help refine the request by asking if there is something specific that the data subject is interested in. This request **must** be copied to the DPO.

   Note:
   If the data subject will not refine the request then all personal data held about them must be collated.

5. **Confirm** – The school administration staff will confirm whether or not the school holds the personal information requested. If no personal data is held (e.g. the data has been disposed of in line with retention guidelines) the DPO must be informed immediately.

   The DPO will then log this and advise the senior administrator to respond to the data subject informing them that the school does not hold personal data about them.

6. **Collate** – Coordinated by the senior administrator, advised by the DPO and assisted by the school IT Support team, the school administration staff will collate the requested data.
   If the collated information includes the personal data of another unrelated data subject that part of the information **must** be redacted. If this is not possible the information must be reformatted such that it does not contain the personal data of other data subjects.

7. **Review** - Once the information is collated the DPO should be contacted to review the collated information. The DPO will check that the collated information corresponds correctly to the subject access request.

8. **Respond** – Once satisfied that the correct personal data has been collated, the DPO will advise the senior administrator to formally respond to the data subject.

   Method of Response

   a. The data subject can be invited to collect their personal information in person, bringing with them two forms of identification that contain their address.

   b. The information can be transferred to them using an encrypted email/file transfer service like "Egress".

   c. If neither of the above means is possible the information can be posted to them by recorded delivery. If this is done the senior administrator should store the delivery certificate with the subject access request.

      Once the response has been made the DPO should be contacted so that the request log can be updated and closed.

Review

This procedure will be reviewed and amended as necessary in the light of a failed subject access response or in line with review of the Data Protection policy.