**Edward Jenner School - Data Protection Policy**

|  |  |  |
| --- | --- | --- |
|  | Date | Signed |
| Date Created | April 2018 | P Brookes |
| Ratified by Head | May 2018 | A Brookes |
| Reviewed and Updated | Sept 20 | P Brookes |
| Reviewed and updated | Oct 22 | A Brookes |
| Next Date of Review | Jan 25 | P Brookes |
| Next Date of Review | Jan 27 |  |

Contents

[Introduction 3](#_Toc51515065)

[1. GENERAL STATEMENT 4](#_Toc51515066)

[2. LAWFUL BASIS FOR PROCESSING PERSONAL INFORMATION 5](#_Toc51515067)

[3. INFORMATION ASSETS 6](#_Toc51515068)

[4. PERSONAL DATA PRIVACY NOTICES 6](#_Toc51515069)

[5. DATA MINIMISATION 6](#_Toc51515070)

[6. ACCURACY 6](#_Toc51515071)

[7. DATA BREACHES 7](#_Toc51515072)

[8. STORAGE LIMITATION 7](#_Toc51515073)

[9. PURPOSE LIMITATION 7](#_Toc51515074)

[10. INTEGRITY, CONFIDENTIALITY AND AVAILABILITY 7](#_Toc51515075)

[11. INFORMATION SHARING 7](#_Toc51515076)

[12. MONITORING 9](#_Toc51515077)

[13. DATA BREACH PROCEDURES 9](#_Toc51515078)

[14. INCIDENT REPORTING 11](#_Toc51515079)

[15. TRAINING 11](#_Toc51515080)

[16. CONSEQUENCES OF A FAILURE TO COMPLY 11](#_Toc51515081)

[17. COMPLAINTS 11](#_Toc51515082)

[18. REVIEW 12](#_Toc51515083)

[19. CONTACTS 12](#_Toc51515084)

[APPENDIX 1- PROCEDURES FOR RESPONDING TO SUBJECT ACCESS REQUESTS MADE UNDER GDPR 2018 13](#_Toc51515085)

[Rights of access to information 13](#_Toc51515086)

[Complying with and Actioning a Subject Access Request 13](#_Toc51515087)

[Complaints 14](#_Toc51515088)

[Contacts 15](#_Toc51515089)

# Introduction

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

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner’s Office (ICO) detailing the information held and its use. These details are then available on the ICO’s website. Schools also have a duty to issue a Privacy Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

**Purpose**

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation (GDPR) 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

**What is Personal Information?**

Personal data is defined in the GDPR as:

*“‘personal data’ means any information relating to an identified or identifiable natural person (‘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”.*

The GDPR refers to the processing of these data as ‘special categories of personal data’. This means personal data about an individual’s:

* race;
* ethnic origin;
* political opinions;
* religious or philosophical beliefs;
* trade union membership;
* genetic data;
* biometric data (where this is used for identification purposes);
* health data;
* sex life; or
* sexual orientation.

**Data Protection Principles**

The principles set out in the GDPR must be adhered to when processing personal data:

* Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
* Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
* Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
* Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
* Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
* Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

# GENERAL STATEMENT

Edward Jenner School is always committed to maintaining the above principles. Therefore, the school will:

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

# LAWFUL BASIS FOR PROCESSING PERSONAL INFORMATION

* 1. Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:
     1. 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 school
     2. 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
     3. Processing is necessary for compliance with a legal obligation to which the data controller is subject
     4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person
     5. Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party
     6. The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters
  2. Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.
  3. The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school’s relevant privacy notice(s). See EJS Information Asset Register for classification of lawful processing decisions.
  4. When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school’s public tasks) a legitimate interest’s assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

# INFORMATION ASSETS

See EJS Information Asset Register

# PERSONAL DATA PRIVACY NOTICES

* 1. Under the provisions of the GDPR 2018 all persons providing personal data involved with the school must be issued with a Data Privacy Notice. This describes the way in which we gather and handle personal data and highlight some of the implications of these processes.
  2. The privacy notices describe:
     1. The categories of personal information that we collect, hold and share include;
     2. Why we collect and use this information at Edward Jenner School:
     3. The lawful basis on which we use this information:
     4. Collecting personal information:
     5. Storing personal data;
     6. Who we share personal information with;
     7. Why we share personal information;
     8. Data collection requirements;
     9. Requesting access to your personal data.

# DATA MINIMISATION

* 1. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
  2. Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.
  3. The School will attempt to maintain a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.
  4. Staff must ensure that data subjects are informed of the period for which data is and how that period is determined in any applicable Privacy Notice.

# ACCURACY

* 1. The school will endeavour to ensure that all data gathered and inputted into our electronic systems is transcribed accurately.
  2. An individual has the right to check the data held about them and to identify any portions that are inaccurate and the right to ensure that any discrepancies are adjusted.

# DATA BREACHES

Data breaches will be dealt with in accordance with EJS Data Breach Procedure document

# STORAGE LIMITATION

* 1. Personal data will be kept securely in accordance with the school’s data protection obligations.
  2. Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained.
  3. Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

# PURPOSE LIMITATION

* 1. Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.
  2. Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

# INTEGRITY, CONFIDENTIALITY AND AVAILABILITY

Staff must maintain data security by protecting the confidentiality, integrity and availabilityof the personal data, defined as follows:

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

# INFORMATION SHARING

From [Keeping children safe in education - GOV.UK (www.gov.uk)](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)

*Information sharing is vital in identifying and tackling all forms of abuse and neglect. As part of meeting a child’s needs, it is important for governing bodies and proprietors to recognise the importance of information sharing between practitioners and local agencies. This should include ensuring arrangements are in place that set out clearly the processes and principles for sharing information within the school or college and with the three safeguarding partners, other organisations, agencies and practitioners as required. School and college staff should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children, whether this is when problems are first emerging, or where a child is already known to the local authority children’s social care.*

* 1. Edward Jenner School is aware of its obligations under the Data Protection Act 2018 and that the GDPR places duties on us to process personal information fairly and lawfully and to keep the information we hold safe and secure.
  2. Edward Jenner School staff have been trained to have due regard to the relevant data protection principles, which allow them to share (and withhold) personal information, as provided for in the Data Protection Act 2018 and the GDPR. Including:
     1. being confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information which is sensitive and personal, and should be treated as ‘special category personal data’.
     2. understanding that ‘safeguarding of children and individuals at risk’ is a processing condition that allows practitioners to share special category personal data. This includes allowing practitioners to share information without consent where there is good reason to do so, and that the sharing of information will enhance the safeguarding of a child in a timely manner but it is not possible to gain consent, it cannot be reasonably expected that a practitioner gains consent, or if to gain consent would place a child at risk.
     3. for schools, not providing pupils’ personal data where the serious harm test under the legislation is met26. For example, in a situation where a child is in a refuge or another form of emergency accommodation, and the serious harms test is met, they must withhold providing the data in compliance with schools’ obligations under the Data Protection Act 2018 and the GDPR. Where in doubt schools should seek independent legal advice.
  3. The Data Protection Act 2018 and GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children.
  4. Further details on information sharing can be found:
     + in Chapter one of [Working Together to Safeguard Children](https://www.gov.uk/government/publications/working-together-to-safeguard-children--2), which includes a myth-busting guide to information sharing
     + at Information [Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers](https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice). The seven golden rules for sharing information will be especially useful
     + at [UK GDPR guidance and resources | ICO](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/) which includes ICO GDPR and guidance from the department
     + in [Data protection: toolkit for schools](https://www.gov.uk/government/publications/data-protection-toolkit-for-schools) - Guidance to support schools with data protection activity, including compliance with the GDPR
  5. Where children leave the school or college, the designated safeguarding lead will ensure their child protection file is transferred to the new school or college as soon as possible, ensuring secure transit, and a confirmation of receipt will be obtained. The file will be transferred separately from the main pupil file. Receiving schools and colleges should ensure key staff such as designated safeguarding leads and SENCOs or the named person with oversight for SEN in a college, are aware as required.
  6. In addition to the child protection file, the designated safeguarding lead will also consider if it would be appropriate to share any information with the new school or college in advance of a child leaving. For example, information that would allow the new school or college to continue supporting victims of abuse and have that support in place for when the child arrives.

# MONITORING

* 1. Authorised IT staff may inspect any IT equipment owned or leased by the school at any time without prior notice.
  2. IT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving the school’s employees or contractors, without consent, to the extent permitted by law. This may be:
     1. to confirm or obtain school business related information;
     2. to confirm or investigate compliance with school policies, standards and procedures;
     3. to ensure the effective operation of school IT;
     4. for quality control or training purposes;
     5. to comply with a Subject Access Request under the GDPR 2018;
     6. to prevent or detect crime.
  3. IT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business related issues retained on that account.
  4. All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the GDPR2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.
  5. Please note that personal communications using school IT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

# DATA BREACH PROCEDURES

* 1. *Notification to the relevant supervisory authority of a breach only need occur where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.* [*UK GDPR guidance and resources | ICO*](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/)

* 1. A 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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
  2. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.
  3. A personal data breach may include:
     + 1. access by an unauthorised third party;
       2. deliberate or accidental action (or inaction) by a controller or processor;
       3. sending personal data to an incorrect recipient;
       4. computing devices containing personal data being lost or stolen;
       5. alteration of personal data without permission; and
       6. loss of availability of personal data.
  4. A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual.
  5. Recital 87 of the GDPR makes clear that ‘when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.’ See Appendix for detailed procedures
  6. The response plan for addressing any personal data breaches that occur is in appendix 1 below
  7. Responsibility for managing breaches is with Mr Phil Brookes
  8. Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.
  9. For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.
  10. Policy breaches may also lead to criminal or civil proceedings.
  11. Edward Jenner School understands that The ICO can serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.
  12. Edward Jenner School understands that The data protection powers of the Information Commissioner’s Office allow it to:
      1. Conduct assessments to check organisations are complying with the Act;
      2. Serve information notices requiring organisations to provide the Information Commissioner’s Office with specified information within a certain time period;
      3. ∙Serve enforcement notices and ‘stop now’ orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
      4. Prosecute those who commit criminal offences under the Act;
      5. Conduct audits to assess whether organisations’ processing of personal data follows good practice,

# INCIDENT REPORTING

* 1. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school’s relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy noncompliance must be reported to the relevant responsible person.
  2. The relevant responsible individual in the school is Mr Phil Brookes.
  3. Written description of the E-Safety Incident must be logged & Infringements and Flowcharts for Managing an E-Safety Incident should be followed (see Appendix A).

# TRAINING

The school will ensure that staff are adequately trained regarding their data protection responsibilities.

# CONSEQUENCES OF A FAILURE TO COMPLY

The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

# COMPLAINTS

Complaints will be dealt with in accordance with the school’s complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

# REVIEW

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher or nominated representative.

The School will undertake an annual review of school records and safe data destruction task. See accompanying document:

***EJS Annual review of school records and safe data destruction checklist***

# CONTACTS

* 1. If you have any enquires in relation to this policy, please contact Mr P Brookes Edward Jenner School, 44 London Road, Gloucester, GL1 3NZwho will also act as the contact point for any subject access requests.
  2. Further advice and information are available from the Information Commissioner’s Office, [Information Commissioner's Office (ICO)](https://ico.org.uk/) or telephone **0303 123 1113** or 01625 545745

# APPENDIX 1- PROCEDURES FOR RESPONDING TO SUBJECT ACCESS REQUESTS MADE UNDER GDPR 2018

# Rights of access to information

From the [Information Commissioner's Office (ICO)](https://ico.org.uk/):

*The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why you are using their data, and check you are doing it lawfully.*

Individuals have the right to obtain the following:

* confirmation that we are processing their personal data;
* a copy of their personal data; and
* other supplementary information provided in a Subject Access Request

# Complying with and Actioning a Subject Access Request

Requests for information must be made in writing, which includes email, and be addressed to Mr Philip BrookesIf the initial request does not clearly identify the information required, then further enquiries will be made.

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

* passport
* driving licence
* utility bills with the current address
* Birth / Marriage certificate
* P45/P60
* Credit Card or Mortgage statement
* *This list is not exhaustive*.

In addition to a copy of their personal data, we will provide individuals with the following information:

* the purposes of your processing;
* the categories of personal data concerned;
* the recipients or categories of recipient we disclose the personal data to;
* the retention period for storing the personal data or, where this is not possible, your criteria for determining how long we will store it;
* the existence of their right to request rectification, erasure or restriction or to object to such processing;
* the right to lodge a complaint with the ICO or another supervisory authority;
* information about the source of the data, where it was not obtained directly from the individual;
* the existence of automated decision-making (including profiling); and
* the safeguards you provide if you transfer personal data to a third country or international organisation.

Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

The response time for subject access requests, once formal identification is received, is 1 calendar month from the request for date has been verified.

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

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

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

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

# Complaints

Complaints about the above procedures should be made to the Proprietor who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school’s complaint procedure.

Complaints which are not appropriate to be dealt with through the school’s complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

# Contacts

If you have any queries or concerns regarding these policies/procedures then please contact Mr Phil BrookesHead of School*.*

Further advice and information can be obtained from the Information Commissioner’s Office, [Information Commissioner's Office (ICO)](https://ico.org.uk/) or **0303 123 1113** or 01625 545745