# Data Protection Policy

## Version V4.0 dated 06/08/24

**Approved by - Under Review/Awaiting Approval Sept 24**
**To be reviewed - Under Review Sept 24**

| DP-24 | UK GDPR-UK Data Protection Policy (v4.0) |
|---|---|

## 1. Introduction




*The UK Data Protection Act 2018 (DPA 18)/UK GDPR defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Personal information is information about a living individual, who can be identified from the information.*

1.1 Empower Trust is committed to protecting the privacy of individuals and handles all personal information in a manner that complies with the DPA18. It is the **personal responsibility** of all employees (temporary or permanent), Governors, contractors, agents and anyone else processing information on our behalf to comply with this policy.

1.2 Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990 and the UK DPA/UK GDPR 2018. All breaches will be investigated and appropriate action taken.

1.3 This policy explains what the school's expectations are when processing personal information and should be read in conjunction with the School Information Security Policy (SISP).

## 2. GDPR Principles

2.1 The UK DPA/GDPR 2018 is supported by a set of 6 principles which must be adhered to whenever personal information is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal information.

2.2 The UK DPA/UK GDPR 2018 principles relevant to the school state that personal information must:

| | | |
|---|---|---|
| **Be processed fairly, lawfully and transparently** | **Obtained for a specified, explicit and legitimate purpose** | **Be adequate, relevant and limited to what is necessary** |
| Be accurate and where necessary up to date | Not be kept longer than is necessary | Be handled ensuring appropriate security |

2.3 There is a further principle called the Accountability Principle. This requires Empower Trust schools to be able to clearly demonstrate their compliance with the UK DPA/UK GDPR 2018. The schools Data Protection Officer undertakes an annual exercise to ensure that the school complies with this principle. See section 12 for further information.

## 3. Access and Use of Personal Information

3.1 Access and use of personal information held by the school, is only permitted by employees (temporary or permanent), Governors, contractors, agents and anyone else processing information on the schools behalf, for the purpose of carrying out their official duties. Use or access for any other purpose is not allowed. Deliberate unauthorised use and access to copying, destruction or alteration of or interference with any personal information is strictly forbidden.

## 4. Collecting Personal Information

4.1 When personal information is collected, for example on a questionnaire, survey or an application form, the 'data subject' (that is the person who the information is about) must be told. This is known as a Privacy Notice.

4.2 Personal information collected, must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where anonymous information would suffice.

4.3 If the information is collected for one purpose, it cannot then be used for a different and unconnected purpose without the data subject's consent unless there is another lawful basis for using the information (see section 5 below). It must be made clear to the 'data subject' all the purposes that their information may be used for **at the time the information is collected,** via a Privacy Notice.

## 5. Lawful Basis for Processing

5.1 When Empower Trust Schools process personal information, it must have a lawful basis for doing so. The UK DPA/UK GDPR 2018 provides a list of 'conditions' when we can process personal and/or 'special category' personal information. This is contained within Article 6 and Article 9 of the regulations ***(see Appendix 1)***.

5.2 The UK DPA/UK GDPR 2018 defines special category personal information as information relating to:

- Race and ethnic origin
- political opinion
- religious or philosophical beliefs
- trade union membership
- processing of genetic/biometric data to uniquely identifying a person
- physical or mental health or medical condition;
- sexual life

5.3 Whenever the school processes personal information, it must be able to satisfy at least one of the conditions in Article 6 of the UK GDPR and when it processes 'special category' personal information; it must be able to satisfy at least one of the conditions in Article 9 of the UK GDPR as well.

5.4 The school can process personal information if it has the data subject's consent (this needs to be 'explicit' when it processes special category information). In order for consent to be valid it must be 'fully informed' which means the person giving consent

must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress and should be recorded. Guidance on how consent should be managed can be found from the school office.

## 6. Disclosing Personal Information

6.1 Personal information must not be given to anyone internally or externally, unless the person giving the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.

6.2 If personal information is given to another organisation or person outside of the school, the disclosing person must identify the lawful basis for the disclosure (see section 4 above) and record their reasoning for using this basis. This record as a minimum should include;

- a description of the information given;
- the name of the person and organisation the information was given to;
- the date;
- the reason for the information being given; and
- the lawful basis.

6.3 If an information sharing agreement or protocol exists, this should be adhered to when providing personal information to others. The agreement/protocol will detail the legal basis for disclosure.

6.4 In response to any lawful request, only the minimum amount of personal information should be given. The person giving the information should make sure that the information is adequate for the purpose, relevant and not excessive. Data minimisation should always be employed.

6.5 When personal information is given either externally or internally, it must be communicated in a secure manner, e.g. password protected/encrypted emails, special delivery or courier, etc.

## 7. Accuracy and Relevance

7.1 It is the responsibility of those who receive personal information to make sure so far as is possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to make sure that it is still accurate and up to date. If the information is found to be inaccurate, steps must be taken to put it right. Individuals who input or update information must also make sure that it is adequate, relevant, clear and professionally worded.

7.2 ‘Data subjects’ have a right to access personal information held about them and have errors corrected. More information about a ‘data subject’s’ rights can be found in Section 9 of this policy.

## 8. Retention and Disposal of Information

8.1 Empowre Trust Schools School hold personal information. The UK DPA/UK GDPR 2018 requires that we do not keep personal information for any longer than is necessary. Personal information should be checked at regular intervals and deleted or destroyed securely when it is no longer needed, provided there is no legal or other business reason for holding it.

8.2 The schools' Information Retention Schedule must be checked before records are disposed of, to make sure that the prescribed retention period for that type of record is complied with. Alternatively advice should be sought from the schools Data Protection Officer.

## 9. Individuals Rights

9.1 Individuals have a number of rights under the UK DPA/UK GDPR 2018. These include:

- **The right to be informed** – See section 4 - Collecting Personal Information
- **The right to access** – A person can ask for a copy of personal information held about them (this is known as a Subject Access request - SAR);
- **The right to rectification** – Personal data can be rectified if it is inaccurate or incomplete
- **The right to erasure** – Person can ask for the deletion or removal of personal data where there is no reason for its continued processing
- **The right to restrict processing** – Person has the right to block or suppress processing of their personal data
- **The right of data portability** – Allows a person to obtain and reuse their personal data for their own purposes
- **The right to object** – A person can object to an organisation processing their personal data for direct marketing, on the basis of legitimate interests or for scientific/historical research and statistics
- **Rights related to automated decision making/profiling** – A person can ask for human intervention in an automated process

9.2 If the school receives such a request on any of the above matters they should seek advice from their Data Protection Officer as soon as the request is received.

9.3 The school has one calendar month in which to respond to a SAR, provided the applicant has clearly stated the nature of their request preferably by completing a subject access request form and suitable proof of identification has been supplied. However the law does allow a SAR to be made verbally. An extension of a further 1-2 months will be applied where a request is deemed complex, the requester should be informed of this within one month of the request being received. The school and Data Protection Officer co-ordinates the processing of all SAR requests. ***See Appendix 2*** for a copy of the SAR form

## 10. Reporting Security Incidents

10.1 The school has a responsibility to monitor all incidents that occur which may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported on a timely basis, investigated and monitored. It is only by adopting this approach that the school can learn from its mistakes and prevent losses recurring. The Data Protection Officer must be informed of an incident/breach within 24 hours of the school becoming aware of the matter.

10.2 Specific procedures have been developed for the reporting of all information security incidents. It is designed to make sure that all relevant information is communicated correctly so that timely corrective action can be taken. The documents below need to be read, understood and followed:

- Information Security Breach Procedure
- Data Breach Investigation

10.3 All employees (permanent, temporary and contractors) must be aware of the procedures and obligations in place for reporting the different types of incidents which may have an impact on the security of the schools information.

## 11. Data Protection Officer

11.1 As the school is a public authority, it has a legal duty to appoint a designated Data Protection Officer.

11.2 The Data Protection Officer has a number of legal duties that they must fulfil including:

- Inform and advise the school of its obligations in respect to data protection
- Monitor compliance with data protection legislation including awareness raising and training of staff
- Provide advice on data protection impact assessments
- Be a contact for the Information Commissioners Office

11.3 The schools current designated Data Protection Officer is Rob Montgomery/Sarah Daffern – IG@telford.gov.uk.

## 12. Accountability

12.1 The DPA 18 requires the school to have appropriate measures and records in place to demonstrate compliance with the act.

12.2 The school demonstrates accountability in a number of ways including:

- Having appropriate policies in place
- Following data protection by design and default
- Using data processing agreements in contracts
- Maintaining records of processing activities
- Implementing technical and organisational security
- Managing data breaches
- Completing data protection impact assessments

- Having an appropriately skilled and knowledgeable Data Protection Officer

**Article 6 Conditions – Personal Data**

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
(b) 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;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject;
(e) 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;
(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. **This shall not apply to processing carried out by public authorities in the performance of their tasks.**

**Article 9 Conditions – Special Category Data**

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

*Appendix 2*

# UK Data Protection Act/ UK General Data Protection Regulations 2018
# Right of Access to Personal Data

## SUBJECT ACCESS REQUEST FORM (SAR)

**Information**

We should respond to your request within one calendar month. Note this can be extended for a further 2 months if the request is deemed complex. However this period does not start until:

a) We are satisfied about your identity
b) You have provided enough detail to locate the information you are seeking

**Please complete the following sections of this form providing as much information as possible to help us deal with your request.**

**1.** Provide details of the person(s) about whom the school is holding data (the Data Subject)

Full Name (Print) _____

Date of Birth _____

| Present Address: | Previous Address (if less than 3 years at your present address): |
|---|---|
| Post Code: | Post Code: |

Telephone Number _____

Email address _____

**2.** Are you requesting information about yourself (person referred to in question 1)? If **YES**, then go to question 3. If **NO** please complete the following:

Full Name (Print) _____

Present Address:

Post Code:

Telephone Number: _____

Email address: _____

Relationship with data subject and brief explanation as to why you are requesting this information rather than the data subject:

_____

_____

***If you are acting on behalf of the data subject you will need to enclose their written authority including a signature or other legal documentation (e.g. power of attorney) to confirm this request. You also need to enclose evidence of your identity and that of the data subject (see section 4 for details of acceptable identity)***

**3.** Please provide a clear description of the information that you are requesting, see table below. **If you provide <u>specific</u> details of what information you want, e.g. name of a document relevant to a time period rather than just the whole of your file you may receive a quicker response.**

| Description of Information | School Staff Member Holding this Information | Time Period for Information Requested |
|---|---|---|
| | | |

4. Please provide **two** pieces of evidence of your identity (one containing a photo). Acceptable types of documents used to verify your identity are detailed below.

| Driving Licence | Passport | National ID Card | Medical Card | Utility Bill |
|---|---|---|---|---|

You may wish to send your documents special/recorded delivery. Your proof of identity will be returned to you securely after verification.

5. All information in respect to your request will be sent to you via secure email unless you make alternative arrangements with the school. We may require further evidence of your identity if you collect your information from school premises.

**Declaration**

To be completed by all applicants. Please note that any attempt to mislead the school may lead to prosecution.

I (insert name) _____

_____

certify that the information given on this application form and any attachments therein to School is accurate and true.

I understand that it is necessary for the [insert] School to confirm my identity and it may be necessary to obtain more information in order to locate the correct information.

Signature _____

Date _____

**Return of the Form**

If you are either posting your documents or hand delivering them then our address is detailed below:

St

Our email address is [in

_____