YSGOL UWCHRADD ABERHONDDU
BRECON HIGH SCHOOL

Data Protection Policy
(General Data Protection Regulation)

Author	**PCC**
Agreed By	**Governors 29/11/2022**
Review Date	**11/2024**

Data Protection Policy Template for Schools

Status	**Version 2**
Guidance Author	**Information Compliance (PCC)**
Date of Issue	**2021**
Date of Previous Issue	**2019**
Review Date(s)	**1. 2021 – 05 – 10** **2. 2021 – 09 – 08**

Table of Contents:

Brecon High School's Data Protection Policy

1. Introduction

1.1. The school collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable 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.

1.2. Schools have a duty to notify the Information Commissioner (The ICO) and to be included in the Register of Data Protection Fee Payers. These details are then available on the ICO's website. As a Public Authority, as defined by the Freedom of Information Act, Schools must designate a Data Protection Officer (DPO) who has been appointed by Powys County Council. Schools also have a duty to issue *a Privacy Notice* to all relevant individuals, which summarises the information held on individuals, why it is held, how long for, the purpose behind collection and the other parties to whom it may be passed on to.

2. Purpose

2.1. This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations 2016 (GDPR) and the Data Protection Act 2018 (DPA), 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 within paper, audio, video or electronic files.

2.2. All staff involved with the collection, processing, disclosure and deletion of personal data must be aware of their duties and responsibilities by adhering to these guidelines. Negligent or malicious non-compliance with this policy may result in disciplinary action being taken.

3. Responsibilities

3.1. The **Head Teacher and Chair of Governors have** overall responsibility for ensuring compliance with this policy and with Data Protection legislation.

3.2. Advice should be sought from the School's DPO on data protection matters as well as reports of data protection breaches.

3.3. **Heads of Departments** are responsible for:

- ensuring that all systems, processes, records and datasets within their area are compliant with this policy and with Data Protection legislation;
- assisting the School's DPO in their duty by providing all information and support where necessary
- ensuring that their staff are aware of their data protection responsibilities.
- consulting the School's DPO on new processing of personal data or issues affecting the use of personal data.
- ensuring that Data Protection Impact Assessments (DPIAs) are undertaken as appropriate on data processing activities within their area (in consultation with the School's DPO).

3.4. **All staff** are responsible for understanding and complying with relevant policies and procedures for handling personal data appropriate to their role and for reporting any breach of personal data held by the School.

4. What is Personal Information?

4.1. Personal information or data is defined as information which relates to an identified or identifiable living individual.

5. Data Protection Principles

5.1. Article 5 of the General Data Protection Regulations 2016 (GDPR) sets out 7 key principles:

- **[1st Principle]** Processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **[2nd Principle]** Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **[3rd Principle]** Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **[4th Principle]** Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **[5th Principle]** Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **[6th Principle]** Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2. The Data Controller shall be responsible for, and be able to demonstrate compliance with, all of the above, otherwise known as the “Accountability principle” and is the **7th principle.**

6. Governance of Data Protection

6.1. The School will maintain oversight and transparency in the management of personal data. The School will meet its accountability duties through the maintenance of the following record keeping systems:

- Up to data privacy notice information for parents, pupils and staff.
- A record of processing activity describing the content, purpose, controls and accountability for each set of records processing personal data.
- A log of information security incidents impacting upon personal data held by the school

7. Data Protection by Design

7.1. The School will apply data protection by design principles to any new systems that results in high-risk processing or those listed by the Information Commissioner.
7.2. All contracts with organisations who are processing personal data on behalf of the School will have GDPR compliant clauses in the contract and be subject to appropriate levels of review and oversight. The contract will clearly set out the expectations for how external contractors and suppliers must handle personal data relating to pupils, their parents and staff.
7.3. There should be consultation with the School's DPO prior to the acquisition or development of new information systems (including the installation of CCTV).
7.4. The School's DPO should be informed and may advise the School that a Data Protection Impact Assessment (DPIA) should be completed in line with the guidance available from the Information Commissioners website: https://ico.org.uk/

8. Data Protection Impact Assessments (DPIAs)

8.1. A DPIA will be conducted when it is determined that the School will be looking to implement a new project or system that processes personal data that is likely to result in a high risk to the rights and freedoms of individuals.
8.2. All risks identified will be recorded within the DPIA as well as mitigations that could be carried out to reduce those identified risks.
8.3. Where the School cannot do anything to reduce a high-level risk, it will consult with the Information Commissioner before implementing the new project or system.
8.4. A log of all DPIAs will be recorded as well as their overall status, i.e. open, closed, abandoned etc.
8.5. The School's DPO will approve and sign off the completed DPIA.

9. Data Accuracy

9.1. All staff must only record personal data that is relevant, accurate and appropriate. This personal data must only be held on School management systems and not on personal notes or devices.
9.2. All IT systems, forms, templates must be reviewed to ensure that by design they are only able to capture the minimum amount of personal data necessary for the activity.

10. Data Retention

10.1. Personal data must not be retained for longer than is necessary for the purpose for which it was gathered. All documents and media containing personal data should be disposed of securely and if possible, using confidential waste methods.

11. Data Protection Rights

11.1. The School will ensure that an individual's rights over their personal data are respected. These rights include:
- The right to be informed that processing is being undertaken;

- The right of access to own personal data and to specific information about the processing;
- The right to object to and prevent processing in certain circumstances;
- The right to rectify or restrict processing of inaccurate data;
- The right to erasure in certain circumstance;
- The right to data portability in some limited circumstances;
- The right to have human input in decisions based solely on automated processing.

11.2. All requests made by individuals relating to their personal data rights should be referred to the Data Manager and undertaken in consultation with the School's DPO. The School must ensure that appropriate action is taken and a response is issued without delay and at least within one calander month.

12. Information Security incidents (including personal data breaches)

12.1. Any information security incidents or personal data breaches that may impact upon the confidentiality, integrity or availability of personal data held by the School must be reported **immediately** to the School's DPO who will action and respond to it accordingly.

12.2. This may include but is certainly not limited to:

- The loss of records, laptops or media containing personal data;
- Unauthorised access to information systems containing personal data;
- Access to personal data with no identified business need;
- Personal data being misdirected to the incorrect recipient;
- Loss of access to systems containing personal data.

12.3. All reported incidents will be recorded to ensure an investigation is undertaken and appropriate mitigation measures are in place and to identify improvements or lessons learnt.

12.4. The School's DPO, in liaison with the School, will consider, where the incident is of sufficient severity or poses a risk to the individual, whether to report the incident to the Information Commissioners Office (ICO). Where the School's DPO determines that an incident constitutes a reportable data breach, then they will report the incident to the ICO and liaise as appropriate.

12.5. If the data breach constitutes a high risk to the data subject then the School will also notify the data subject.

13. General Statement

13.1. The school is committed to maintaining the above principles at all times. Therefore, the school will in summary:

- 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 (SARs).
- Set out procedures to ensure compliance with Article 16 of the GDPR where the individual has the right to obtain rectification of inaccurate personal data concerning them. Additionally allowing the data subject to have incomplete personal data completed including by means of providing supplementary statement (these should be reported to the School's DPO for advice and assistance).
- Set out procedures to ensure compliance with Article 17 of the GDPR where the individual has the right to obtain the erasure of personal data concerning him or her in certain circumstances (these should be reported to the School's DPO for advice and assistance).
- Set out procedures to ensure compliance with Article 18 of the GDPR where the individual has the right to obtain the restriction of processing in certain circumstances (these should be reported to the School's DPO for advice and assistance).
- Ensure staff are aware of and understand policies and procedures.

14. Complaints

14.1. Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling should be referred to the School's DPO who will advise the School accordingly and who may contact the ICO.

15. Review

15.1. 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 DPO (School's), Headteacher, or nominated representative.

16. Contacts

16.1. If you have any enquires in relation to this policy, please contact the Headteacher via bhs@brecon-hs.powys.sch.uk or 01874 622361 who will also act as the contact point for any Subject Access Request (SAR).

16.2. Further advice and information is available from the Information Commissioner's Office, Home | ICO or telephone 0303 123 1113 or 029 2044 8400 for the Wales Regional Office.

17. Appendix 1 – Subject Access Requests

17.1. There are two distinct rights of access to information held by Schools about pupils.
17.2. Under the GDPR any individual has the right to make a request to access the personal information held about them.
17.3. The right of those entitled to have access to curricular and education records as defined within the Educational (Pupil Information) (Wales) Regulations 2011.
17.4. These procedures relate to subject access requests (SAR's) made under the General Data Protection Regulations 2016 (GDPR):

18. Actioning a Subject Access Request

18.1. Requests for information must be made in writing, which includes email, and be addressed to (insert name of Headteacher). If the initial request does not clearly identify the information required, then further enquiries will be made.
18.2. 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.

18.3. 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.
18.4. If the information requested is **only** the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.
18.5. The response time for SAR, once officially received, is one calendar month **(not working or school days but calendar days, irrespective of school holiday periods)**. However, the time will not commence until after receipt of identification or clarification of information sought.
18.6. 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.

18.7. Schools are required to log and monitor the number of requests received and the timescales involved.

19. Subject Access Request Exemptions.

19.1. The GDPR and DPA allows exemptions as to the provision of some information; **therefore, all information will be reviewed prior to disclosure**. Advice and assistance should be sought from the School's DPO.

19.2. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the statutory timescale.

19.3. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

19.4. 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.

19.5. 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.

20. SAR Complaints

20.1. Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

20.2. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Data Protection Officer (School's) and Information Commissioner. Contact details of both will be provided with the disclosure information.

21. Appendix 2 – Requests for Rectification/Erasure/Restriction

21.1. The School's procedure for complying with a request for rectification or erasure of personal data or the right to restrict processing or to object to processing made under the GDPR.

21.2. Requests for information must be made in writing; which includes email, and be addressed to the Headteacher. If the initial request does not clearly identify what is required, then further enquiries will be made.

21.3. The identity of the requestor must be established before the undertaking and request, 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.

21.4. Full consideration must be given to the request. All such requests must be considered after consultation with the DPO (School's) who will advise on the correct process. Please note that there is NO automatic right to rectification/erasure/restriction of processing or objecting to processing.

21.5. Where the school has forwarded the personal data to other data controllers then all reasonable steps should be taken to advise those controllers that the data subject has requested one of the above.

21.6. The School must communicate any decision regarding the rectification, erasure or restriction of personal data to the data subject within one month of receipt of request.

End of Policy.