Ysgol Uwchradd Y Frenhines Elisabeth

Queen Elizabeth High School

Moving Forward Together

DATA PROTECTION POLICY

Part 1 – Handling Personal Information

Part 2 – Breach Reporting

Part 3 – Privacy Notice

Part 4 – Freedom of Information

Date established by Governing Body: 23rd May 2018

Responsible Person – Mr Dave Williams

Designated role – Acting Head Teacher

Chair of Governors signature – Helen Starkey

Date – 23/05/2018

If you require this document in an alternative format please contact - Email – dpo@qehs.carms.sch.uk

Policy Version Control

Version	Date	Page	Section	Reason for review	Summary of amendment	Chair of Governor's signature

Part 1

Information Governance

Handling Personal Information

Policy & Procedure

Contents

1. Introduction

1.1 Queen Elizabeth High School collects and uses a wide range of personal data about our pupils and staff in order to deliver education and pastoral care. If we fail to take adequate care of the personal data we deal with and it is lost, stolen, disclosed inappropriately or otherwise misused, this could have a serious impact on the individuals concerned ranging from distress to actual physical harm. Personal information is therefore a valuable asset, but also a liability if we handle it incorrectly.

1.2 This policy and procedure is therefore designed to ensure that personal information is handled securely, in particular its storage and transfer, to assist in complying with the School's legal obligations.

2. Definition of personal information

2.1 Personal information or data is any information that relates to a living individual, who can be identified from the information, directly or indirectly.

2.2 In practice, this is likely to include a very wide range of data, including, but not limited to:

- Names, addresses and dates of birth
- Reference numbers such as Unique Pupil Numbers
- Personal financial information such as bank details
- Descriptive or biographical information regarding an individual
- Photographs or other images

2.3 The terms personal information and personal data are used throughout this policy and procedure and have the same meaning.

2.4 There are also special categories of personal information and we must be particularly careful when dealing with these. The special categories are personal information regarding:

- Racial or ethnic origin
- Political Opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Genetic data
- Biometric data
- Health
- Sex life or sexual orientation

2.5 There are also specific requirements for information relating to criminal convictions and offences.

3. Legal background

3.1 Data Protection legislation sets out rules relating to the processing of personal data. Processing is defined as collecting, recording, storing and making any use of personal data, including its disclosure and disposal.

3.2 We are required to observe six principles relating to the processing of personal data. The sixth principle sets out a specific requirement that appropriate technical or organisational measures must be used to protect against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data.

3.3 The consequences of not handling personal data correctly could have serious consequences for the School, as administrative fines of up to €20,000,000 can be imposed for serious Data Protection breaches.

4. Policy statements

4.1 Queen Elizabeth High School is committed to processing personal information in accordance with the requirements of Data Protection legislation.

4.2 The School views the proper handling of personal data as essential in delivering our services and maintaining the confidence of the people that we deal with.

4.3 Any personal data held by the School which is not in the public domain will always be treated as being strictly confidential.

4.4 The School will make maximum use of secure electronic methods to store and transfer personal data.

4.5 This policy is approved by, and has the full support of, the Governing Body of the School.

5. Scope

5.1 This policy and procedure applies to all personal data owned by the School.

5.2 This policy and procedure applies to all employees of the School, including:

- Temporary employees and agency workers
- Volunteers
- Contractors acting as data processors

6. Responsibilities

6.1 School employees are responsible for:

- Protecting the personal information they process by adhering in full to this policy and procedure.

6.2 Headteachers are responsible for:

- Ensuring that their employees are made aware of this policy and procedure and have understood its requirements
- Ensuring that the requirements of the policy and procedure are fully implemented within the School and staff
- Ensuring that their employees have received appropriate training on Data Protection requirements
- Taking appropriate action when breaches of the policy and procedure occur

6.3 Breaches of this policy and procedure may lead to disciplinary action being taken against the employees responsible.

7. Use of portable devices, removable media and cloud storage

7.1 Portable devices include, but are not limited to:

- Laptop computers & tablets
- Smartphones

7.2 Removable media include, but are not limited to:

- USB memory sticks/storage devices
- SD cards
- CD-Roms and DVDs

7.3 Personal information must not be processed on removable media that are not owned by the School.

7.4 Personal information must not be processed on portable devices that are not owned by the School unless an appropriate control supplied by the School is in place.

7.5 Portable devices or removable media must only be used to collect, store, transport or transfer personal information when there is a genuine need to do so and there is no alternative method available.

7.6 Before using portable devices or removable media to collect, store, transport or transfer personal information, permission must be obtained from the Headteacher, Deputy Head or Head of Year.

7.7 Personal data must never be kept on portable devices or removable media unless it is encrypted.

7.8 Portable devices or removable media containing personal information must be stored and transported securely.

8. Secure storage of personal information

8.1 Paper records, portable devices and removable media containing personal information must be kept securely within School premises. This will involve keeping them in locked cupboards when not in use and ensuring that keys are not accessible to unauthorised persons. Adequate building security must be in use.

8.2 Storage of personal data in paper records should be minimised where possible.

8.3 Within School premises, personal data must not be left unattended where anyone can have access to it, such as on desks, window sills, corridors, printers and photocopying machines.

8.4 Personal information must not be processed on computer equipment that is not owned by the School.

8.4 Personal data processed on office based computers must be password protected and should never be left visible on a screen if the computer is unattended.

8.5 Personal information processed on computers must never be stored on the hard disk of the computer. This protects the data in the event of computer failure or theft.

8.6 Personal data must never be uploaded/stored in cloud storage not provided by the School. This includes, but is not limited to:

- Personal email accounts (such as Gmail, Hotmail)
- Dropbox
- Microsoft OneDrive

8.7 When personal information is displayed on computer screens used in a public area, it must not be visible to pupils or visitors to the School.

9. Taking personal information out of the School

9.1 Personal information must not be taken out of School premises unless it is absolutely necessary to do so and only with the permission of the relevant manager or the Headteacher, Deputy Head or Head of Year.

.

9.2 When paper records, portable devices or removable media containing personal information are taken out of office premises, they must be kept secure, carried safely and never be left unattended where they can be accessed by unauthorised persons such as within vehicles or in areas accessible to the public.

9.3 Paper records containing personal information must only be taken home with the permission of the Headteacher, Deputy Head or Head of Year, who is responsible for ensuring that a suitable working environment including a means of securely storing papers such as a lockable drawer or cabinet is available. A record should be kept of what information is taken off site, when it has been taken, by whom and when it is returned.

9.4 Paper records must not be kept in the home for longer than necessary and returned to the office premises at the earliest opportunity.

9.5 Family members, or any other unauthorised persons, must not be allowed access to any personal information, in any format, which is taken home.

10. Transferring personal information outside the School

10.1. This includes sending personal data to the following:

- The Welsh Government
- Other Schools
- Carmarthenshire County Council and other local authorities
- External agencies, companies and organisations solely for the discharge of educational activities
- Parents and pupils

10.2 Personal information must only be sent outside the School where this is in accordance with the law and it is absolutely necessary to do so.

10.3 Personal data must not be provided to any external organisation when anonymised or statistical information could be used as an alternative. Any personal information we do provide should be relevant and the minimum necessary for a specified purpose.

10.4 The School will never share personal information for commercial gains

11. Using an electronic method to transfer information

11.1 The safest and quickest way of transferring personal information outside the School is a secure electronic method. This must always be considered as the first option and used whenever possible. Such methods could include, but are not limited to:

- The Common Transfer System/School2School

- Sending email using a secure email system such an Egress Switch
- Sending the information via a secure email network such as Zimbra, where the sender and recipient both have accounts
- Sending email via Zimbra to Carmarthenshire County Council email addresses

11.2 When using secure email, sending to groups or lists of contacts should be avoided as this introduces the risk of disclosing personal information to recipients who are not authorised to access it. The same care has to be taken when replying to emails, as choosing the 'reply to all' option may also result in the information being sent to unintended and unauthorised recipients.

11.3 When beginning to type an email address, several similar addresses that have been used previously will often be suggested by the email software. It is essential that the correct address is chosen before the message is sent.

11.4 Clear instructions must be included as to how the recipient is to handle the information, for example, if it is not to be passed on without first contacting the sender.

11.5 When a secure electronic method is not available and the information is not sensitive personal data, or otherwise likely to cause damage or distress if disclosed to a third party, then it can be sent by standard email without the need for any further assessment of risk. An example would be responding to an individual's correspondence about a prominent issue already in the public domain. Care must nonetheless be taken to ensure that the information is sent to the correct email address.

12. Using other methods to transfer personal data

12.1 Other methods of transferring personal data include but may not be limited to:

- Royal Mail
- Courier
- Hand delivery/collection

12.2 When a secure electronic method is not available and the information is not sensitive personal data, then it can be sent by Royal Mail without the need for any further assessment of risk. An example would be a letter informing a person that they have been successful in their job application. We also need to routinely send letters containing personal information to our customers, for example, in connection with benefit claims. Care must nonetheless be taken to ensure that the information is correctly addressed to a named recipient.

12.3 In the absence of a secure electronic method, when the information to be sent is sensitive personal information, then the following must always be considered when deciding what means of transfer is appropriate:

- The precise nature of the information, its sensitivity, confidentiality or value
- What damage or distress could be caused to individuals if the information was lost or accessed by unauthorised persons
- The effect any loss would have on the School
- The urgency of providing the information, taking into account the effect of not sending the data, or any delay in sending the data

12.5 If it is considered appropriate to send sensitive personal information by Royal Mail, the following steps must be taken:

- The envelope in which the information is sent must be clearly addressed to a named recipient
- The information must be sent by a traceable method

12.6 When using a courier to transport any personal information, steps must be taken to ensure that they operate within appropriate security standards.

12.7 When it is not deemed appropriate to transfer personal information by Royal Mail, or courier and a secure electronic method is not an option, the information should be provided by hand to the recipient, or an arrangement made for the data to be collected and a record kept which includes:

- A brief description of the information provided
- When it was provided
- The name and contact details of the recipient, and if relevant, their designation

12.8 Where it is considered necessary, records containing personal data should include a watermark stating “Disclosed Copy”. This could include cases where pupil records are disclosed to parents.

13. Checking information before it is sent

13.1 When sensitive personal data, or personal information that is otherwise likely to cause damage or distress if disclosed to a third party, is being sent outside the School in any format, the sender should consider having the information checked by another person before it is sent.

13.2 The person sending the information is responsible for:

- Ensuring that the email or postal address the information is being sent to is correct
- Making sure that when information is supplied in hard copy, a named recipient of the information is clearly specified
- Ensuring that no information relating to third parties has been included in error, either in a letter/email or an attached document

13.3 If it is considered necessary for another person to check the information, the other person is responsible for:

- Checking that the email or postal address the information is being sent to is correct
- When information is being supplied in hard copy, checking that a correct named recipient of the information has been specified
- Checking that no information relating to third parties has been included in error, either in a letter/email or an attached document
- Recording that they have checked the email, letter and/or attachments

15. Retention of personal information

15.1 When it is no longer necessary to keep personal data on portable devices or removable media, it should be deleted immediately.

15.2 Where a portable device is used for the purpose of collecting personal information, the information should only be kept on it for as long as is absolutely necessary. The information should be saved on the School's network at the earliest opportunity and deleted off the device.

15.3 In all other cases, where it is decided that it is no longer necessary to retain personal information, the **Information & Records Management Society Toolkit for Schools** must be referred to before deleting or destroying records.

15.4 Paper records containing personal information must be disposed of securely, by shredding or the use of the confidential waste service in accordance with the **School's Records Disposal Procedure.**

15.5 Disposal of IT equipment must only be carried out by the Council's IT Services in accordance with the Council's **Information Security Policy. (Checking with County if this is included in our SLA)**

16. Breaches of security

16.1 These would include cases where personal data is lost or stolen, either in electronic or paper format. Other examples would include emailing personal data to an unintended recipient or accidentally placing personal data on the School's website.

16.2 All security breaches must be reported immediately to the School's Data Protection Officer.

16.3 Failure to report, or delay in reporting, security breaches can have potentially serious consequences for data subjects, staff, other individuals and the School.

17. Ensuring equality of treatment

17.1 This policy and procedure must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion or belief, age, sex, gender identity, sexual orientation, parental, marital or civil partnership status.

Part 2

Information Governance

Breach Reporting & Response Policy

Contents

1. Purpose

1.1 This Policy sets out Queen Elizabeth High School requirements for ensuring that personal data breaches are reported and responded to in a timely and effective manner.

1.2 Data Protection legislation places an obligation on the School to document all personal data breaches, in effect, to maintain an internal register of such incidents.

1.3 The School is also required report breaches which are likely to result in a risk to the *"rights and freedoms"* of individuals to the Information Commissioner's Office (ICO) and in certain cases, inform the individuals whose personal data has been affected.

2. Scope

2.1 This policy applies to all employees of the School, including:

- Temporary employees and agency workers
- Volunteers
- Contractors acting as data processors

2.2 The legal definition of the term breach, as used in this policy, is as follows:

"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."

This policy therefore covers incidents where the confidentiality, integrity or availability of personal data, in any format, is compromised.

2.3 Examples of breaches include, but are not limited to:

- Loss or theft of ICT equipment such as laptops, tablet devices, smartphones, USB drives containing personal data
- Loss or theft of paper records, such as files, individual documents, notebooks containing personal data
- Loss or theft of financial information such as payment card details
- Accidental disclosure of information such as emails or letters sent to the wrong recipients and containing personal data
- Accidental deletion of records, affecting service delivery and potentially impacting on individuals' wellbeing
- Unauthorised access to IT systems, cyber and ransomware attacks

3. Reporting breaches

3.1 Breaches are most likely to come to light as a result of:

- A complaint or representation by a member of the public or external organisation
- Staff becoming aware of an issue during the course of their duties
- A data processor informing the School of an incident

3.2 In order to ensure that breaches can be acted upon they should be reported by employees to the Headteacher or Deputy Head immediately.

3.3 Out of School hours, breaches must be reported as soon as possible at the beginning of the next working day.

3.4 To support independence of investigation of any expected breach, a Governing Body Breach Committee will be formed and if appropriate, an individual with specific skills and experience who is independent of the school, will be co-opted onto that committee.

This committee will comprise of the:

- Chair or Vice Chair of the Governing Body
- Any two members of the Governing Body, on a rota

4. Procedure for responding to breaches

4.1 The response to a breach will follow the following steps:

- Containment and recovery
- Assessment of risk
- Notification of a breach (where necessary)
- Evaluation and response

4.2 Upon being made aware of a breach, the Head teacher or his nominee will complete the Breach Report template (attached as **Appendix 1**) and notify the Data Protection Officer and the chair of the Governing Body Breach Committee.

4.3 The Head teacher will be responsible for initiating an immediate investigation into the cause(s) of the breach and identifying and implementing necessary containment & recovery actions, which must be clearly documented in the Breach Report. Examples of such actions include, but are clearly not limited to:

- Attempting to locate and retrieve lost paper records
- Finding a missing item of ICT equipment
- Ensuring that a wrongly addressed email has been deleted
- Informing the Police in the event of a theft
- Changing door access codes

4.4 The Head teacher will then undertake an assessment of the risk(s) posed by the breach and record this in the Breach Report. This assessment must take into account:

- The type of data involved, its nature, sensitivity and volume
- Whether the subject(s) could be harmed by the breach, for example, identity theft, fraud or damage to reputation
- Who the individuals are, for example, children or other vulnerable
- The number of individuals' personal data affected

4.5 Once these steps have been completed and recorded, the Breach Report will be forwarded to the Governing Body Breach Committee and referred to the Data Protection Officer (DPO).

4.6 The DPO will then determine whether it is necessary to notify the ICO of the breach, taking into consideration the circumstances as documented. In the event that notification is required, the Governing Body Breach Committee will provide the ICO with all of the information required under Data Protection legislation.

4.7 Based on the assessment of risk, the Data Protection Officer, in consultation with the Head teacher and the Governing Body Breach Committee will then determine whether the data subject(s) affected by the breach are to be notified**.** Where this is deemed necessary, the information to be communicated to the subject, set out in Data Protection legislation, must be provided in full.

4.8 The steps set out from 4.1 to 4.7 above must be completed as soon as practicable, but in any event within a maximum of 10 working days

4.9 Finally, in consultation with the Head teacher, the Governing Body Breach Committee will identify and document any further recommendations and actions required. For example, if the breach was caused by systemic and ongoing problems, then actions such as the following may be necessary:

- Changes to procedures and systems
- Review of policies
- Staff training/awareness

5. Other policies or procedures

5.1 Where a reported breach constitutes a breach of any other School policies, then the requirements of the relevant policy will be followed, which may include initiating disciplinary procedures.

5.2 Where the breach constitutes a complaint, a response to the complainant will be provided in accordance with the **School's Complaints Procedure**.

6. Compliance measurement

6.1 Compliance with this Policy is mandatory. Breaches of this policy by staff may lead to disciplinary action being taken.

7. Sponsor

7.1 This Policy is owned by Queen Elizabeth High School.

8. Custodian

8.1 It is the responsibility of the Head teacher and Data Protection Officer to ensure that this policy is reviewed and updated.

9. Ensuring equality of treatment

9.1 This policy and procedure must be applied consistently to all irrespective of race, colour, nationality, ethnic or national origins, language, disability, religion or belief, age, sex, gender identity, sexual orientation, parental, marital or civil partnership status.

Part 2 - Appendix 1

PERSONAL DATA BREACH REPORT

Reference:

1. Full details of the breach

2. Containment & recovery action(s) taken
3. Assessment of ongoing risk
Type of data involved:
Number of data subject(s) affected:
Number of records affected:

Risk(s) to data subject(s):
Risk(s) to School:

4. Notification of breach required?
Information Commissioner's Office:
Data subject(s):

5. Evaluation & response – recommendations & action(s) required

6. Other considerations (including HR issues)

Head teacher	
Date	

Recipients
DPO:
Governing Body Breach Committee:
Other:

Part 3

Privacy notice for Queen Elizabeth High School

How we use your information

The proper handling of personal information by the School is very important in delivering education to our pupils.

Personal data is any information that relates to a person who can be directly or indirectly identified from the information. The terms ‘information’ and ‘personal data’ are used throughout this privacy notice and have the same meaning.

To ensure that the School treats personal information correctly, we seek to adhere in full to the requirements of Data Protection legislation.

This privacy notice has therefore been produced to explain as clearly as possible what we do with personal data.

1. The purposes for which we use personal data

The information we collect about you and your child will be used for the purposes of:

- Supporting your child’s learning
- Monitoring and reporting on their progress
- Providing appropriate pastoral care
- Assessing the quality of our education

The legal basis for the processing of the personal data is to comply with our legal obligations under the Education Acts 1944 to 2014.

If you do not give us the information we need when we ask for it, this could have an impact on your child’s education and safety.

2. What type of information do we use?

We collect the following types of personal data:

- Contact details for you and your child
- Your child’s date of birth
- Your child’s gender
- Unique Pupil Number
- Unique Learner Number
- Your family’s composition
- Child’s language ability
- Education details
- Images/photographs as part of our school activities
- Information about your child’s health
- Your child’s racial or ethnic origin
- Biometric data

We also use a CCTV system in the school to record images. This is to keep your child and our employees safe.

Where applicable, we will collect and use the following:

- Free school meals eligibility
- Additional Learning Needs
- Whether a pupil child is Looked After by a local authority

3. Do we use information received from other sources?

The School collects information directly from you but we also receive information from the following sources:

- Any previous schools your child has attended
- Carmarthenshire County Council Education & Children Services department
- Other local authorities
- The NHS

The following types of personal data are obtained:

- Unique Pupil Number
- Pupil ID
- Contact details for you and your child
- Your family's composition
- Language ability
- Education details
- Images/photographs
- Information about your child's health
- Your child's racial or ethnic origin
- Religious or philosophical beliefs in faith schools

4. Transferring information abroad

Personal data about you and your child will not be transferred outside the United Kingdom.

5. Who has access to the information we use?

We share pupil information with the following recipients:

- Carmarthenshire County Council
- Welsh Government
- Other schools
- Education through Regional Working regional consortium
- Hywel Dda University Health Board
- Alps and Fisher Family Trust who analyse pupil data for the School
- Learner Record Service
- Careers Wales
- Examination bodies

- External agencies, companies and organisations solely for the discharge of educational activities

The school will never share personal information for commercial gains

Capita, who provide our Management Information System can have access to personal data when they carry out maintenance work on the system.

Information relating to our pupils is also hosted by Ceredigion County Council on Carmarthenshire County Council's Management Information System.

There are other specific situations where we may be required to disclose information about you, such as:

- Where the Council is required to provide the information by law
- Where disclosing the information is required to prevent or detect a crime
- Where disclosure is in the vital interests of the person concerned

6. How long we will keep personal data

We keep personal data in accordance with guidelines published by the Information & Records Management Society: www.irms.org.uk

7. Your Data Protection rights

You have the right to:

- Obtain access to the personal data that the school is processing about you
- Have any inaccurate or incomplete information rectified (corrected)
- Withdraw your consent to processing, where this is the only basis for the processing
- Make a complaint to the Information Commissioner's Office (ICO), the independent body in the UK which protects information rights

In some circumstances, you may have the right to:

- Object to the processing of your personal information
- The erasure of your personal data
- Restrict the processing of your personal information
- Data portability

You can also access your child's education record under the Pupil Information (Wales) Regulations 2011.

8. Contact details

For more information regarding this privacy notice and your rights, please contact our Data Protection Officer at: Queen Elizabeth High School
Email: ncooke@qehs.carms.sch.uk Tel: 01267 245300

Contact details for the Information Commissioner's Office along with further guidance on Data Protection legislation can be found on the ICO website: www.ico.org.uk

Part 4

Freedom of Information - Policy Statement

The school responds to requests for information under the Freedom of Information Act in line with latest statutory guidelines. The school will seek data protection guidance from the designated Local Authority Officer with regards to exemptions.

If appropriate, the school will make reasonable charges to cover costs. This will be agreed with the requestor prior to any information being provided.