CEFN SAESON COMPREHENSIVE SCHOOL

DATA PROTECTION POLICY

Contents

April 2018

1. Cefn Saeson Governing Body [hereinafter referred to as “the Governing Body”] is committed to ensuring its compliance with the requirements of the Data Protection Act 1998, General Data Protection Regulations and the forthcoming Data Protection Act 2018 (‘the Legislation’). We recognise the importance of personal data to our organisation and the importance of respecting the privacy rights of individuals. This Data Protection Policy (‘the Policy’) sets out the principles which we will apply to our processing of personal data so that we not only safeguard one of our most valuable assets, but also process personal data in accordance with the law.

2. It is the responsibility of all our employees to assist the Governing Body to comply with this Policy. In order to help employees comply, we have produced a Data Protection Policy Guidance Note (‘the Guidance’) which explains in more detail the requirements of the Legislation. Employees must familiarise themselves with both this Policy and the Guidance and apply their provisions in relation to any processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal. Furthermore, serious breaches of the legislation could also result in personal criminal liability for the staff concerned.

3. In addition, a failure to comply with this Policy could expose the business to enforcement action by the Information Commissioner (which could result in restrictions being imposed on our use of personal data) or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

4. For the purpose of this policy:

Data	means information which – (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or (e) is recorded information held by a public Governing Body and does not fall within any of paragraphs (a) to (d).
Data Controller	means … a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor	in relation to personal data, means any person (other than an employee of the data controller)

	who processes the data on behalf of the data controller.
Data Subject	means an individual who is the subject of personal data.
Inaccurate Data	means information or data that is incorrect or misleading as to any matter of fact.
Personal Data	means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Processing	in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including – (a) organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.
Recipient	in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.
Sensitive Personal Data	means personal data consisting of information as to - (a) the racial or ethnic origin of the data subject,

	(b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
Third Party	means any person other than – (a) the data subject, (b) the data controller, or (c) any data processor or other person authorised to process data for the data controller or processor

Data protection principles

5. The Governing Body will comply with the following principles in respect of any personal data which it processes as a data controller. It must be:

5.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

5.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

5.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

5.4 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;

5.5 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; personal data may be stored for longer periods insofar as the personal data will be processed solely

for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

5.6 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."

Basis of Processing

6 The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever the Governing Body process personal data:

6.1 **Consent:** the individual has given clear consent for the Governing Body to process their personal data for a specific purpose.

6.2 **Contract:** the processing is necessary for a contract the Governing Body have with the individual, or because they have asked the Governing Body to take specific steps before entering into a contract.

6.3 **Legal obligation:** the processing is necessary for the Governing Body to comply with the law (not including contractual obligations).

6.4 **Vital interests:** the processing is necessary to protect someone's life.

6.5 **Public task:** the processing is necessary for the Governing Body to perform a task in the public interest or for the Governing Body's official functions, and the task or function has a clear basis in law.

6.6 **Legitimate interests:** the processing is necessary for the Governing Body's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if the Governing Body is a public Governing Body processing data to perform the Governing Body's official tasks.)

Accountability

7. The Governing Body must

7.1 implement appropriate technical and organisational measures that ensure and demonstrate that we comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.

7.2 maintain relevant documentation on processing activities;

7.3 appoint a data protection officer;

7.4 implement measures that meet the principles of data protection by design and data protection by default. Measures could include data minimisation, pseudonymisation or transparency;

7.5 allowing individuals to monitor processing; and

7.6 creating and improve security features on an ongoing basis.

7.7 use data protection impact assessments where appropriate.

External Arrangements

8. Where the Governing Body passes personal data to any external organisation, officers must ensure a Data Processing Agreement is in place. Suitable Data Processing Agreement can be obtained from the Legal Services Section.

9. In addition, any external contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the Governing Body. Specific terms must also be included and advice should be sought from the Legal Services Section in this regard.

Information Asset Registry

10. One of the requirements of the Legislation is to maintain a record of all the processing activities that take place within the Governing Body. For this, we need to identify:

10.1 what personal data we process;

10.2 what is the lawful basis for processing;

10.3 how we store and keep the data secure;

10.4 who has access to it;

10.5 who we share the data with and what sharing agreements are in place;

10.6 how long we keep it for.

11. The Governing Body has a dedicated Information Asset Registry which must be completed for all information that is held within each of the Governing Body's Directorates.

Data Protection Officer

12. The Governing Body has appointed …… as the Data Protection Officer.

13. The role of the Data Protection Officer includes

13.1 Information and advising officers of the Governing Body of their data protection obligations

13.2 monitoring compliance of policies and procedures. This includes monitoring responsibility and training of staff involved in data processing.

13.3 ensuring the Information Asset Registry is an active registry that identifies all systems that hold personal data

13.4 advising on the necessity of Data Protection Impact Assessment, the manner of their implementation and data breach reporting

13.5 serve as contact point for individuals on privacy matters, including subject access requests

Additional Requirements

14. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

15 Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

16. This Policy may be amended from time to time to reflect any changes in legislation.

DATA PROTECTION POLICY

GUIDANCE NOTE

1. INTRODUCTION

1.1 This Guidance Note ('the Guidance') forms part of the Data Protection Policy and provides supplementary information to enable employees to better understand and comply with the Data Protection Policy.

1.2.1 Cefn Saeson Governing Body [hereinafter referred to as "the Governing Body"] is required to comply with the Data Protection Act 1998, General Data Protection Regulations and Data Protection Act 2018 ('the Legislation') in respect of its processing of personal data (such as information about our customers, clients/service users, employees and contractors/suppliers). It is important for all employees to familiarise themselves with both the Data Protection Policy and this Guidance so that any processing of personal data can be carried out in accordance with the Legislation.

1.2.2 The Governing Body should be aware that there is other legislation regulating public access to information such as the Freedom of Information Act 2000 which sometimes must be read in conjunction with the Legislation.

1.3 The Governing Body must comply with its obligations under the Legislation. In order to do this the Governing Body must comply with the Data Protection Policy and this Guidance whenever the Governing Body process personal data, as well as any other data protection related policy that may be applicable to the Governing Body's area of work.

ANY FAILURE TO COMPLY WITH THIS POLICY MAY BE A DISCIPLINARY OFFENCE WHICH COULD RESULT IN DISMISSAL. NEGLIGENT OR DELIBERATE BREACHES OF THE LEGISLATION COULD ALSO RESULT IN CRIMINAL LIABILITY FOR THE GOVERNING BODYPERSONALLY.