Arolygiaeth Ei Mawrhydi dros Addysg a Hyfforddiant yng Nghymru
Her Majesty's Inspectorate for Education and Training in Wales

Access to Information Policy

This policy is also available in Welsh.

Information sheet

For further advice contact: Data Protection Officer

Date of publication: July 2021

Version control

Document version	Author	Date of issue	Changes made
1.0	Alison Palmer	January 2007	
2.0	Alison Palmer	May 2011	Routine review
3.0	Ben Thomas	28 November 2011	Initial draft for consultation
4.0	Information Governance Group	14 April 2014	Includes removal of £10 fee for a subject access request introduction of environmental regulations and general update of FOI policy
4.1	Dai Williams	27 August 2015	Review and update logo, content and execute an EIA.
4.2	Information Governance Group	06 August 2018	Review following introduction of GDPR.
5.0	Information Governance Group	July 2021	Tone of voice amendments made as a result of policy review – also updating of information regarding legislation, streamlining of information regarding subject access requests (and separating form from policy), and adding further contact information details.

Equality Impact Assessment

A business rationale assessment has been carried out and this policy contributes to Estyn's strategic objectives and delivery principles.

In accordance with Estyn's Equality Impact Assessment, an initial screening impact assessment has been carried out and this policy is not deemed to adversely impact on the grounds of the nine protected characteristics as laid out by the Equality Act 2010.

Contents	Page

Introduction

Policy statement

1 The General Data Protection Regulation 2016 (GDPR) describes how data and information about people should be handled. It is supplemented by the Data Protection Act 2018, which replaced the Data Protection Act 1998, and is the UK's implementation of GDPR. The GDPR and 2018 Data Protection Act include the right for people to access their personal data. They set out rules for processing personal information and apply to personal data held in structured manual files as well as data stored electronically.

2 The Freedom of Information Act 2000 (FOIA) gives a general right of access to all types of 'recorded' information held by public authorities, subject to certain exemptions, and places a number of obligations on public authorities. The exemptions are designed to protect confidential or other information where disclosure may prejudice the interests of the State or of third parties.

3 The FOIA, GDPR and the DPA come under the heading of information rights and are regulated by the Information Commissioner's Office (ICO).

4 Our publication scheme has been developed using the ICO's best practice model. We update it regularly, for example when a new policy is introduced or an existing one is updated.

5 The Environmental Information Regulations 2004 (EIR) specifically provide public access to environmental information held by public authorities.

6 This policy sets out the arrangements that we have in place to ensure compliance with the above Acts and Regulations.

Scope of this policy

7 We are committed to full compliance with the GDPR. GDPR applies to electronic and manual filing systems where personal data is accessible according to specific criteria. Personal data covers both facts and opinions about an individual.

8 We are committed to full compliance with the FOIA. The main features of the FOIA that impact on our work are:

- facilitating a general right of access to information that we hold in the course of carrying out public functions, subject to certain conditions and exemptions
- information must be disclosed, unless the public interest in maintaining the exemption outweighs the public interest in disclosure
- adopting a publication of information scheme. The scheme must be approved by the Information Commissioner, and will specify the classes of information that we intend to publish, how we will to publish it, and whether the information is available to the public free of charge or for a fee.

9 We are committed to full compliance with the EIR. The EIR provide public access to environmental information held by us in two ways:

- we must make environmental information available proactively
- as a member of the public you are entitled to request environmental information from us

10 The EIR apply only to the environmental information that we hold. The FOIA gives people access to most other types of information we hold.

General Data Protection Regulations 2016

What are the principles of the GDPR?

11 We shall be responsible for, and be able to demonstrate, compliance with the data protection principles that set out the main responsibilities for organisations to ensure that data is:

a) processed lawfully, fairly and in a transparent manner in relation to individuals
b) collected for specified, explicit and legitimate purposes and not further processed in way that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not be considered to be incompatible with the initial purposes
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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
f) 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 and considering further technological developments, including encryption, when assessing implementing any new security measures

In addition, the data controller is responsible for, and able to demonstrate compliance with, the above principles, and ensures that appropriate processes and records are in place to demonstrate compliance.

What type of information is protected by the GDPR?

12 **Personal data** - any information relating to a person where someone can be directly or indirectly identified with the data. For example: names, dates of birth, addresses, emails, employment details, financial details, preclusions, class or year details, and educational outcomes.

13 **Sensitive personal data** - for example: race, ethnic origin, sexual orientation, safeguarding information, political and religious views, health information (e.g. additional learning needs).

14 Personal data relating to criminal convictions and offences are not considered sensitive personal data, but similar extra safeguards might apply when this information is processed.

Making a request for your personal data

15 Under the GDPR, you will have the right to:

- confirmation that your data is being processed
- access to your personal data
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

16 GDPR allows you to access your personal data so that you are aware of and can verify the lawfulness of how your data is processed. This is known as the 'right of access'.

17 In certain circumstances, where personal data is processed electronically, you will be able to ask for a copy of your personal data in a structured, electronic format. You can also ask that your personal data is transferred to another organisation or business.

18 We must provide information within at least one month of receiving your request. This can be extended by a further two months if requests are complex or numerous. If we need to extend the deadline, we will contact you within one month of receiving of the request to explain why the extension is necessary.

19 Requests are free, however if your requests are noticeably unfounded, excessive or repetitive, we can:

- charge a fee to cover the administrative costs of providing the information, or
- refuse to respond.

20 Where we refuse to respond to a request, we will explain why and will advise you of your right to complain to the supervisory authority and to a judicial remedy within at least one month.

21 Your request must:

- be made in writing (preferably by completing a Subject Access Request)
- provide evidence of your identity
- clearly describe the information you are requesting

22 If you think that the information we hold about you may also identify another person, you may want to get that person's agreement to allow you to receive such information and send it with your application.

23 If you are a current member of Estyn staff and with to make a request regarding information about yourself, please contact Human Resources in the first instance, who will be able to advise you of the process.

24 Where we process a large quantity of information about you, the GDPR allows us to ask you to specify what information your request relates to.

25 We have a duty to make sure that the information we hold about individuals is accurate and up to date. However, if you identify that we hold incorrect or incomplete information about you then you have the right to request that we correct the data. We will do this no later than 30 days after your request, Unless we consider your request is unfounded or excessive. We may also add an extra statement to your record to clarify information. When your information has been corrected, any incorrect information will be deleted.

Exemptions from the GDPR

26 There are exemptions from the regulations to accommodate special circumstances you can read more about these on the Information Commissioner's website.

Lawful basis for processing personal data under the GDPR

27 You must have a valid lawful basis in order to process personal data. There are six lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual. Most lawful bases require that processing is 'necessary'. The lawful bases are:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose

b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations)

d) Vital interests: the processing is necessary to protect someone's life

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

f) Legitimate interests: the processing is necessary for your 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 you are a public authority processing data to perform your official tasks)

28 Once an organisation has established a lawful basis, then this must be documented in a privacy notice.

29 The lawful basis identified directly affects which of the rights an individual is able to exercise in respect of the data..

Who has rights and obligations under the GDPR?

30 The GDPR provides the following rights for individuals:

1 The right to be informed
2 The right of access
3 The right to rectification
4 The right to erasure
5 The right to restrict processing
6 The right to data portability
7 The right to object
8 Rights in relation to automated decision making and profiling.

31 The Regulation protects the rights of the individuals the data is about (data subjects), mainly by placing duties on those who decide how and why such data is processed (data controllers). A list of terms, their meaning and significance can be found below:

32 '**Processing**' relates to anything done with data, including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

33 A **data subject** means an individual who is the subject of personal data. For us this will include, for example, staff, additional inspectors, peer assessors/inspectors, independent inspectors, and any personal details captured during inspections or surveys.

34 A **data controller** determines the purposes for which and the way in which any personal data is, or will be, processed.

35 A **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 and in accordance with their instructions. Our data processors would include, the Welsh Government as part of service level agreements, contractors and partners.

36 The **Information Commissioner** is an independent office-holder appointed by the Crown to administer and enforce the General Data Protection Regulation 2016, the Freedom of Information Act 2000 and other legislation governing the use of, and access to, information. The Information Commissioner is independent of government and reports directly to Parliament.

37 An **information notice** is a legal document which the Information Commissioner can issue to a data controller, requiring them to supply information to the Commissioner so that they can assess whether or not the data controller is complying with the General Data Protection Regulation or Freedom of Information Act.

38 The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

39 We must comply with the accountability principle. The accountability principle in Article 5(2) of the GDPR requires us to demonstrate that we comply with the principles and state explicitly that this is our responsibility. This means that we must:

- implement appropriate technical and organisational measures that ensure and demonstrate compliance. Including internal data protection policies, staff training, internal audits of processing activities, and reviews of internal HR policies
- consider further technological developments, including encryption, when assessing implementing any new security measures
- maintain relevant documentation on processing activities
- appoint a data protection officer
- implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
  a) data minimisation
  b) pseudonymisation
  c) transparency
  d) allowing individuals to monitor processing
  e) creating and improving security features on an ongoing basis
- use data protection impact assessments where appropriate

Roles and responsibilities

40 As Accounting Officer of Estyn, **Her Majesty's Chief Inspector** has overall responsibility for information governance in Estyn. They are ultimately responsible for determining the policies that apply to the information we hold. The Accounting Officer provides assurance, through the annual Governance Statement, that all risks to us and to the information we hold are effectively managed and mitigated.

41 Estyn's **qualified person** is a role that can be delegated by Her Majesty's Chief Inspector to members of our senior management team. The qualified person makes judgements about prejudice to the effective conduct of public affairs, in relation to requests for us to release information. Within Estyn, this will usually be a Strategic Director.

42 **Strategic Directors** are responsible for making sure the information held in their areas of responsibility fully complies with the policies and procedures set by the Chief Inspector. This includes information processed by contractors, partners or other bodies working under a service level agreement.

43 **Managers** are responsible for making sure that the staff they manage are aware of our policies, procedures and guidance, and for checking that staff understand apply policies, procedures and guidance appropriately in carrying out their day to day work.

44 **All staff** are responsible for processing information in line with our policies, procedures, guidance and our information governance framework.

45 The **Data Protection Officer** is responsible for overseeing the policies and procedures that apply to GDPR, FOIA and EIR. They also provide advice to our staff on data protection issues.

46 **Information Officers (IO GDPR & IO FOI)** are responsible for managing all requests for disclosure of personal data and all requests for access to information that we receive. They are supported by the Information Administrator and Case Officers. The IO GDPR will provide advice directly to staff on data protection where possible. The IO FOI will provide advice on FOI matters, or will refer the issue to a person such as an Information Asset Owner (IAO) for advice.

47 **Case Officers** are responsible for administering allocated GDPR or FOI cases. They are the main point of contact and advice for individual cases; they co-ordinate the process to retrieve and documents that are requested, and they provide a full response to the person making the request.

48 An internal working group may be called together to discuss and provide advice to case officers on individual cases. Members of this group include corporate services staff with GDPR or FOIA experience. The group is chaired by the IO GDPR or IO FOI.

49 The **Information Technology Cyber Security Officer** (ITCSO) is responsible for data security incident management in consultation with Estyn's Data Protection Officer.

Training

50 We will provide training for all staff about this policy and any related procedures and guidance. The training will be appropriate for each person's grade and responsibilities.

51 Our staff must read our Information Governance framework policies and confirm they have read and understood them. All staff handle protected personal data as part of their jobs, and they must complete the Civil Service 'Responsible for Information' training every three years.

52 We will also make sure that contractors or anyone working under contracts, service level agreements and partnership agreements are aware of their responsibilities to us as data processors. We will ensure they have measures in place to ensure that they can competently carry out their responsibilities.

53 Where necessary, for example IT services, contractors should make sure that staff or any other person engaged by them in connection with a contract signs a confidentiality agreement.

54 Contracted Additional Inspectors (CAIs) must follow our records retention policy for any information relating to the inspections they take part in. CAIs must acknowledge their responsibility to comply with these requirements when they accept inspection contracts.

Monitoring, review and evaluation

55 We keep a register of all the data disclosure requests that we receive. We also keep a register of all requests for access to information made under the FOIA and EIR, as

well as the action taken for each application. The IO FOI monitors this register, and reports on it to the Senior Management Team.

56 We have procedures for reviewing our arrangements for administering and managing personal data. These procedures include systems for auditing our compliance with the Acts and those who process data on our behalf.

57 We register all complaints received about our data protection, FOI and EIR arrangements, and use any learning points that some from these complaints to improve our data protection policies, procedures and guidance.

58 We will review this policy to make sure that it is up to date and effective, and that it reflects emerging good practice and new legal directions.

Feedback and complaints

59 If you are not satisfied with the decision on your request for information under GDPR, FOIA or EIR, you are entitled to ask us to review the decision. Your request for a review should be sent to the Complaints Manager within 20 working days of the date on our decision letter. Our response to your subject access request will be reviewed by a senior manager.

60 For more information, please read our feedback and complaints procedure.

Definitions of the Freedom of Information Act and Environmental Information Regulations 2004

Timescales

61 If you make a request for information under the FOIA or the EIR, we will respond to you no later than 20 working days after we receive your request.

62 Some exceptions to this timescale are if:

- we have to transfer the request to another public authority because we do not hold the information you have requested; the 20-day deadline starts when they receive your request
- the request is unclear

63 In these cases, the 20-day deadline starts when the other authority receives your request, or when your clarify your request.

64 There may also be an extension if:

- we have to apply a public interest test, which allows us to extend the timescale (this does not apply to exceptions under the EIR)
- a fee is payable, and a fees notice is sent to you within the 20 working days

Exemptions/exceptions and the public interest test

65 The FOIA and the EIR give rights of public access to information held by public authorities. FOIA has a number of exemptions that allow public authorities to withhold some or all of the information requested, where a justifiable reason exists. EIR have a number of exceptions that allow public authorities to refuse to provide requested information, again where a justifiable reason exists.

66 If the exemption is qualified, our qualified person must weigh the public interest in maintaining the exemption (or an exception in the case of EIR) against the public interest in disclosure. This means that they must decide whether the public interest is better served by maintaining the exemption and withholding the information, or by disclosing the information. Further guidance can be found on the ICO website.

Exemptions under FOIA

67 **Absolute Exemptions** – If an absolute exemption applies, the information does not have to be released under FOIA and the public interest test does not apply.

Section 21	Information reasonably accessible to applicant by other means
Section 23	Information supplied by, or relating to security bodies
Section 32	Information contained in court records, etc.
Section 34	Parliamentary privilege
Section 36	Effective conduct of public affairs (applying only to

	information held by House of Commons or House of Lords)
Section 40	Information is personal data
Section 41	Information provided in confidence
Section 44	Prohibitions on disclosure

68 **Qualified Exemptions** - even if one of the following exemptions applies, the information must be disclosed unless the public interest in withholding it is greater than the public interest in releasing it.

Section 22	Information intended for future publication
Section 24	National security exemption
Section 26	Defence
Section 27	International relations
Section 28	Relations within the United Kingdom
Section 29	The economy
Section 30	Investigations
Section 31	Law enforcement
Section 33	Audit Functions
Section 35	Policy formulation
Section 36	Effective conduct of public affairs (excluding matters covered under the absolute exemption at S 36)
Section 37	Communications with Her Majesty and the awarding of honours
Section 38	Health and safety
Section 39	Environmental information accessible via EIRn
Section 42	Legal professional privilege
Section 43	Commercial interests

Exceptions under EIR

69 EIR contains exceptions from the duty to make information available, but there is a presumption in favour of disclosure. Some of the exceptions relate to categories of information, for example unfinished documents and internal communications. Others are based on the harm that would arise from disclosure, for example if releasing the information would adversely affect international relations or intellectual property rights. There is also an exception for personal data if providing it would be contrary to the General Data Protection Regulation.

70 Under Part 3, EIR, a public authority may refuse to disclose environmental information requested if:

a) an exception to disclosure applies under paragraphs 12(4) or 12(5)
b) in all the circumstances of the case, the public interest in maintaining the exception outweighs the public interest in disclosing the information

12(4)	A public authority may refuse to disclose information to the extent that:	
	(a)	it does not hold that information when an applicant's request is received
	(b)	the request for information is manifestly unreasonable
	(c)	the request for information is formulated in too general a

		manner and the public authority has complied with regulation 9
	(d)	the request relates to material which is still in the course of completion, to unfinished documents or to incomplete data
	(e)	the request involves the disclosure of internal communications.
12(5)	Where disclosure would adversely affect:	
	(a)	international relations, defence, national security or public safety
	(b)	the course of justice, fair trial, criminal or disciplinary inquiry
	(c)	intellectual property rights
	(d)	the confidentiality of proceedings of a public authority where confidentiality is provided by law
	(e)	the confidentiality of commercial or industrial information where confidentiality is provided by law to protect a legitimate economic interest
	(f)	the interests of person who provided information where that person:
		(i) was not under, and could not have been put under, any legal obligation to supply it to that or any other public authority
		(ii) did not supply it in circumstances where the public authority is entitled to disclose the information apart from these regulations to disclose it and
		(iii) has not consented to its disclosure
	(g)	the protection of the environment to which the information relates
13		Personal data of third parties

Fees

71 We will meet the majority of costs for complying with requests for information under the FOIA and EIR. However, we have the right to refuse to answer requests for information if the cost of complying would exceed the 'appropriate limit', as set out in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.

72 When we estimate the cost of complying with a request for information, we will take into account the staff time (a rate of £25 per hour) involved in finding out whether we hold the information, locating and retrieving any documents which contain the information, and extracting the information from these documents.

73 Where we estimate the cost to be below £450 (the 'appropriate limit'), there will be no charge.

74 If it would cost us more than £450 to comply with the request, we can refuse it outright or do the work for an extra charge. In these cases, we will contact you to discuss whether you would prefer to modify your request to reduce the cost.

75 We don't generally provide information in response to requests that will cost more than £450. If we do decide to comply with such a request, we will charge for the cost of compliance as described above, plus:

- communication costs
- £25 an hour for staff time taken for printing, copying or sending the information

VAT will be charged at the normal rates.

76 Where we choose to charge for information published through our publication scheme or a request for access to information, we will send you a fees notice as required by section 9 of the FoI Act. You will be required to pay any fees within a period of 3 months, starting with the day we send you the fees notice.

77 If we receive two or more related requests within a period of 60 consecutive working days from a single individual or from two or more individuals who appear to be acting together or in pursuance of a campaign, we will combine the costs of complying with these requests. If the combined estimated costs of complying are in excess of £450, we will not be obliged to comply with any of the requests.

78 Where a request for information is a mixed request (for example if it contains a request for personal information and environmental information), we will respond to each part separately. There is no charge for providing personal information to the subject of that information under the terms of the GDPR. Charges for environmental information will be made under the terms of Part 2, section 8 of the EIR.

Making a request under FOIA

79 Your request must:

- be in writing (by email or letter)
- include your name
- include an address for correspondence
- clearly describe the information you are requesting

Making a request under EIR

80 You can make requests verbally or in writing, but as we must respond to all requests in writing we will need your name and contact details for correspondence. We will check with you that we have understood the information you've requested.

How to contact us

Access to information

81 **Email**: enquiries@estyn.gov.wales

Write to: Information Officer
Estyn
Anchor Court
Keen Road
Cardiff
CF24 5JW

Phone: 02920 446446

More information

Information Commissioner's Office

82 For independent advice about access to information and data protection, you can contact the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Phone: 0303 123 1113 or 01625 545745
Email: casework@ico.org.uk

83 For more information on General Data Protection Regulation, Freedom of Information Act and Environmental Information Regulations, visit the ICO website https://ico.org.uk