## **Definition**

## In this policy, ‘we’, ‘us’ and ‘our’ means In Our Element.

In this policy ‘staff’ means all employed, contracted or volunteer members.

**1. Aims**

We aim to ensure that all personal data collected about staff, learners, parents, clients’ other individuals is collected, stored, and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

**2. Legislation and Guidance**

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) on the GDPR.

**3. Definitions**

|  |  |
| --- | --- |
| **Term**  | **Definition**  |
| Personal data  | Any information that relates to an identified or identifiable natural person. This may include:* Name (including initials)
* Location data

It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural, or social identity. |
| Special categories of personal data  | Personal data, which is more sensitive and so needs more protection, including information about: * Racial or ethnic origin
* Religious or philosophical beliefs
* Genetics
* Health – physical or mental
 |
| Processing  | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.  |
| Data subject  | The identified or identifiable individual whose personal data is held or processed.  |
| Data controller  | A person or organisation that determines the purposes and the means of processing of personal data.  |
| Data processor  | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.  |
| Personal data breach  | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.  |

**4. The data controller**

In Our Elementprocesses personal data relating to staff, learners, parents, clients’, and others, and therefore is a data controller.

In Our Element has paid its data protection fee to the ICO, as legally required.

**5.Roles and responsibilities**

This policy applies to **all staff** working within, In Our Element. staff who do not comply with this policy may face disciplinary action.

**5.1 Data protection officer (DPO)**

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is also the first point of contact for the ICO.

Our DPO is Martyn Griffiths who can be contacted on 07843 591601 or martyn@inourelement.org.uk

**5.2 All staff**

Staff are responsible for:

* Collecting, storing, and processing any personal data in accordance with this policy
* Completing training every 2 years
* Informing In Our Element of any changes to their personal data, such as a change of address
* Contacting the DPO in the following circumstances:
* With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
* If they have any concerns that this policy is not being followed
* If they are unsure whether they have a lawful basis to use personal data in a particular way or not
* If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
* If there has been a data breach
* Whenever they are engaging in a new activity that may affect the privacy rights of individuals
* If they need help with any contracts or sharing personal data with third parties

**6. Data protection principles**

The GDPR is based on data protection principles that we must comply with.

The principles say that personal data must be:

* Processed lawfully, fairly and in a transparent manner.
* Collected for specified, explicit and legitimate purposes.
* Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed.
* Accurate and, where necessary, kept up to date.
* Kept for no longer than is necessary for the purposes for which it is processed.
* Processed in a way that ensures it is appropriately secure.

This policy sets out how In Our Element aims to comply with these principles.

**7. Collecting personal data**

**7.1 Lawfulness fairness and transparency**

We will only process personal data where we have one of 5 ‘lawful bases’ (legal reasons) to do so under data protection law:

* The data needs to be processed so that we can **fulfil a contract** with the individual, or the individual has asked us to take specific steps before entering a contract.
* The data needs to be processed so that we can **comply with a legal obligation.**
* The data needs to be processed to ensure the **vital interests** of the individual or another person i.e., to protect someone’s life.
* The data needs to be processed for the **legitimate interests** of In Our Element or a third party, provided the individual’s rights and freedoms are not overridden.
* The individual (or their parent/carer in the case of a learner under 12 years old) has freely given clear **consent.**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

* The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent.**
* The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security, or social protection law.**
* The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
* The data has already been made **manifestly public** by the individual.
* The data needs to be processed for the establishment, exercise, or defence of **legal claims.**
* The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
* The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
* The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
* The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

* The individual (or their parent/carer in the case of a pupil under 12 years old) has given **consent.**
* The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
* The data has already been made **manifestly public** by the individual.
* The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise, or defence of **legal rights.**
* The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

**7.2 Limitations, minimisation, and accuracy.**

We will only collect personal data for specified explicit and legitimate reasons.

Staff must only process personal data where it is necessary to do their jobs and comply with policy and lawful instruction from the DPO.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with, In Our Element’s record retention schedule.

**8. Sharing personal data**

We will not share personal data with anyone else without prior consent, but there are certain circumstances where we may be required to do so without requiring consent. These include, but are not limited to, situations where:

* There is an issue with a learner or parent/carer that puts the safety of our staff at risk.
* We need to liaise with other support agencies – we will seek consent as necessary before doing this.
* Our suppliers or contractors need data to enable us to provide services to our staff and learners – for example, IT companies. When doing this, we will:
* Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
* Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
* Only share data that the supplier or contractor needs to carry out their service.
* We will also share personal data with law enforcement and government bodies where we are legally required to do so.
* We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our learners or staff.
* Where we transfer personal data internationally, we will do so in accordance with data protection law.

**9. Subject access requests and other rights of individuals**

**9.1 Subject access requests**

Individuals have a right to make a ‘subject access request’ to gain access to personal information that the IOE holds about them. This includes:

* Confirmation that their personal data is being processed.
* Access to a copy of the data.
* The purposes of the data processing.
* The categories of personal data concerned.
* Who the data has been, or will be, shared with.
* How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period.
* Where relevant, the existence of the right to request rectification, erasure, or restriction, or to object to such processing.
* The right to lodge a complaint with the ICO or another supervisory authority.
* The source of the data, if not the individual.
* Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
* The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

* Name of individual
* Correspondence address
* Contact number and email address.
* Details of the information requested.

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

**9.2 Children and subject access requests**

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil’s ability to understand their rights will always be judged on a case-by-case basis.

**9.3 Responding to subject access requests.**

When responding to requests, we:

* May ask the individual to provide 2 forms of identification.
* May contact the individual via phone to confirm the request was made.
* Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
* Will provide the information free of charge.
* May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:

* Might cause serious harm to the physical or mental health of the learner or another individual
* Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child’s best interests.
* Would include another person’s personal data that we can’t reasonably anonymise, and we don’t have the other person’s consent and it would be unreasonable to proceed without it.
* Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, negotiations, or confidential references.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

**9.4 Other data protection rights of the individual**

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

* Withdraw their consent to processing at any time.
* Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
* Prevent use of their personal data for direct marketing
* Object to processing which has been justified on the basis of legitimate interests.
* Be notified of a data breach (in certain circumstances)
* Make a complaint to the ICO.
* Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances)
* Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

**10. Parental requests to see the educational record**

Learners over 12 may make their own requests, or parents can complete a valid request for access if they have the correct permission from their child to do so.

A response will be provided within 30 working days.

This applies if the learner concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the learner or another individual.

**11. Photographs and video**

As part of our activities, we may take photographs and record images of individuals.

Parents/ learners are asked to complete a consent form for the use of photographs and video before any In Our Element sessions begin. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further, however it may not be possible to undistributed images and videos, though we will do our reasonable best to do so.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Such uses may include:

* Sharing with learner’s school (where consent has been given).
* Used by In Our Element for publicity or marketing (where consent has been given).

**12. Data security and storage of records**

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage.

**13. Disposal of records**

Personal data that is no longer needed will be disposed of securely.

**14. Personal data breaches**

In Our Element will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

**15. Training**

All staff are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or In Our Element’s processes make it necessary.

**16. Monitoring arrangements**

This policy is owned by In Our Element and will be reviewed every 2 years.

In Our Element is responsible for monitoring and reviewing this policy.

**17. Links with other policies and documents.**

This data protection policy is linked to our:

* Staff employment contract
* Records and retention policy

**How to complain**

If you have any concerns about our use of your personal information, you can make a complaint to:

Martyn Griffiths

In Our Element

7 Troed Y Bryn Terrace

Penycae

Swansea

SA9 1YJ

martyn@inourelement.org.uk

You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO’s address:

Information Commissioner’s Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>

**Appendix 1. Personal data breach procedure**

This procedure is based on guidance on personal data breaches produced by the Information Commissioner’s Office (ICO).

On finding or causing a breach, or potential breach, the staff member must immediately notify the DPO.

Martyn Griffiths

martyn@inourelement.org.uk

**The breach must be recorded on the GDPR.co.uk website.**

The DPO, will investigate the report, and determine whether a breach has occurred. The DPO will consider whether personal data has been accidentally or unlawfully:

* Lost
* Stolen
* Destroyed
* Altered
* Disclosed or made available where it should not have been.
* Made available to unauthorised people.

Staff will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is likely that is the case, the DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff should help the DPO with this where necessary, and the DPO should take external advice when required. (See the actions relevant to specific data types at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.

The DPO will work out whether the breach must be reported to the ICO, and the individuals affected using the ICO’s self-assessment tool.

The DPO will document the decisions (either way) in case it is challenged later by the ICO, or an individual affected by the breach.

Where the ICO must be notified, the DPO will do this via the ‘report a breach’ page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the awareness of the breach. As required, the DPO will set out:

A description of the nature of the personal data breach including, where possible:

* The categories and approximate number of individuals concerned.
* The categories and approximate number of personal data records concerned.
* The name and contact details of the DPO
* A description of the likely consequences of the personal data breach
* A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Where the DPO is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

* A description, in clear and plain language, of the nature of the personal data breach
* The name and contact details of the DPO
* A description of the likely consequences of the personal data breach
* A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

* Facts and cause
* Effects
* Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be securely stored.

**Actions to minimise the impact of data breaches.**

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it’s appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save, or replicate it in any way.

The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school/ client should inform any, or all, of its local safeguarding partners.