GDPR Data Protection

Purpose of policy
We are committed to ensuring that we comply with the six data protection principles and the other requirements of GDPR, as follows:

1. we will process personal data lawfully, fairly and in a transparent manner;
2. we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
3. we will only process the personal data that is adequate, relevant and necessary for the relevant purposes;
4. we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;
5. we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; and
6. we will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Personal Data
Zems Academy will only collect and process personal data if one of the conditions set out below has been satisfied:

- the express consent of the data subject is obtained prior to the processing of personal data. Consent must be freely given; it must also be specific and informed. It must be given by an unambiguous statement or by clear affirmative action signifying the data subject's agreement to the processing. In practice this means that wherever possible consent should be obtained in writing and signed by the subject with clear wording in plain English explaining precisely what they are agreeing to. Where written consent is not possible, verbal consent can be given but the terms of the consent must be clearly given to the subject and a written record of the consent kept;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering the contract;
- processing is necessary for compliance with a legal obligation to which Zems Academy is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the purposes of the legitimate interests pursued by Zems Academy or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Except where the processing is based on consent, Zems Academy will satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

Zems Academy will document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles and will include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices

Where sensitive personal data is processed, also identify a lawful special condition for processing that information (see section below), and document it.

Sensitive Personal Data
Sensitive personal data (sometimes referred to as 'special categories of personal data') are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Zems Academy may from time to time need to process sensitive personal data. We will only process sensitive personal data if we have a lawful basis for doing so and one of the special conditions for processing sensitive personal data applies, e.g.:

- the data subject has given explicit consent;
- the processing is necessary for the purposes of exercising the employment law rights or obligations of Zems Academy or of the data subject;
- the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
- the processing relates to personal data which are manifestly made public by the data subject;
- the processing is necessary for the establishment, exercise or defence of legal claims; or
- the processing is necessary for reasons of substantial public interest.

Policy statement
Zems Academy needs to collect and use certain types of information about people we deal with in order to operate. These include current, past and prospective employees, stakeholder organisations, members of the public, suppliers and others.

Zems Academy is also required by law to collect and process personal information in order to meet its task as a training provider. This personal information is handled with the utmost care and attention – whether on paper, electronically, or other means. Zems Academy is committed to full compliance with the applicable data protection legislation including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (referred to as the "GDPR") and all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003.

Zems Academy has a commitment to:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff who handle personal data, so that they can act confidently and consistently
- Notify the Information Commissioner voluntarily, even if this is not required

Zems Academy regards the fair and lawful processing of personal information as essential in order to successfully achieve its objectives and ensure the support and confidence of the general public and stakeholders.

Key risks
Data Security

Zems Academy will take appropriate technical and organisational security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We have proportionate procedures and technology to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Where Zems Academy uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. Personal data will only be transferred to another party to process on our behalf (a data processor) where a GDPR-compliant written contract is in place with that data processor.

Storage and Retention of Personal Data

Zems Academy will maintain data security by protecting the confidentiality, integrity and availability of the personal data.

Our security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas should be reported.
- Secure desks, cabinets and cupboards. Desks and cupboards should be locked if they hold personal data.
- Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed.
- Equipment. Screens and monitors must not show personal data to passers-by, and should be locked when unattended. Excel spreadsheets will be password protected.
- Personal Devices. Anyone accessing or processing Zems Academy's personal data on their own device, must have and operate a password only access or similar lock function, and should have appropriate anti-virus protection. These devices must have Zems Academy's personal data removed prior to being replaced by a new device or prior to such individual ceasing to work with Zems Academy.

Personal data (and sensitive personal data) will not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained.

Personal data (and sensitive personal data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Data Breaches

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal data is stored;
- unauthorised access to or use of personal data either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

If anyone believes personal data held by Zems Academy has been compromised in some way they MUST report this immediately to the Data Protection Officer via email at Belal@zems.org.uk.

Zems Academy will;
- investigate any reported actual or suspected data security breach;
- where applicable, make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

Responsibilities

Company Directors
Company Directors have overall responsibility for ensuring that Zems Academy complies with its legal obligations.

Data Protection Officer
Zems Academy will appoint a Data Protection officer, whose responsibilities will include:
- Briefing the Board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on tricky Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification to the ICO
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

Senior Leadership Team
With the guidance and advice of the DPO, the Senior Leadership Team is responsible for the management of personal data, ensuring good practice and that compliance with DP legislation can be demonstrated. This includes:
- development and implementation of this policy;
- security and risk management in relation to compliance with this policy;
- having data protection expertise;
- undertaking an annual review of personal data held to ensure that there is a sound business reason for holding that information.

Directors and senior managers have equivalent responsibility and accountability for the control of personal data within their area of responsibility.

The DPO has specific responsibilities for designing procedures and will provide staff with clarification on any aspect of DP legislation and compliance.

Employees & Volunteers
All staff and volunteers will be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees and volunteers.)

Compliance with DP legislation is the responsibility of all employees who control or process personal data.

Employees are responsible for ensuring that their own personal data is accurate and up to date.

Enforcement
Zems Academy takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal data is being processed;
- carries the risk of significant civil and criminal sanctions for the individual and the College; and
- may in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under Zems Academy's procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

Training
Employee's need to be adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Security
Arrangements in regard to data security are covered by Information Security Policy.

Data recording and storage
Arrangements in regard to data recording and storage are covered by Information Security Policy.

Right of Access

Responsibility
It is the responsibility of the Data Protection Officer (DPO) to ensure that right of access requests are handled within the legal time limit which is one month

Procedure for making request
Data subjects have the right to access personal data that the Zems Academy holds about them. Such a request must be made in writing and follow the process set out below. There is a responsibility on all employees to pass on anything which might be a subject access request to the DPO without delay.

Requests must be;

- processed by the DPO or suitably trained deputy;
- confirmed that the data subjects are who they say they are and have a right of access to the information;
- checked to ensure that any third party data subject's rights are not overlooked;
- respond to requests without undue delay and in any event within one month of receipt;
- recorded accurately.

It is also possible that the Zems Academy may also receive request from a data subject to erase personal data, rectify inaccurate data, restrict/cease or not begin processing personal data. All such requests or notices must be referred to the DPO and responded to either by;

- agreeing to comply with the request; or
- giving the reasons why the request is regarded as unjustified, either wholly or in part.

Provision for verifying identity

Where the person managing the access procedure does not know the individual personally there will be appropriate checks undertaken to establish the identity of the person making the request before handing over any information. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

***This list is not exhaustive.**

Charging

In general requests for information will be provided free of charge. However Zems Academy reserves the right to charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. Zems Academy may also charge a reasonable fee to comply with requests for further copies of the same information. The fee will be based on the administrative cost of providing the information.

Transparency

Commitment

Zems Academy is commitment to ensuring that data subjects are aware that their data is being processed and

- for what purpose it is being processed
- what types of disclosure are likely, and
- how to exercise their rights in relation to the data

Data subjects have the following rights in relation to their personal data:

- to be informed about how, why and on what basis that data is processed
- to obtain confirmation that their data is being processed and to obtain access to it and certain other information, by making a subject access request
- to have data corrected if it is inaccurate or incomplete;
- to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten')
- to restrict the processing of personal data where the accuracy of the information is contested, or the processing is unlawful (but the data subject does not want the data to be erased), or where Zems Academy no longer needs the personal data but the data subject requires the data to establish, exercise or defend a legal claim
- to restrict the processing of personal data temporarily where the data subject does not think it is accurate (and Zems Academy is verifying whether it is accurate), or where the data subject has objected to the processing (and Zems Academy is considering whether the College's legitimate grounds override the data subject's interests).

For further information on how these individual rights can be exercised contact should be made in writing with Zems Academy's Data Protection Officer.

Lawful Basis

Underlying principles

In relation to any processing activity that involves personal data we will, before the processing starts for the first time and then regularly while it continues:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis for that processing, i.e.:
    - that the data subject has consented to the processing;
    - that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - that the processing is necessary for compliance with a legal obligation to which Zems Academy is subject;
    - that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
    - that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority by Zems Academy; or
    - where Zems Academy is not carrying out tasks as a public authority, that the processing is necessary for the purposes of the legitimate interests of Zems Academy or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices; and
- where sensitive personal data is processed, also identify a lawful special condition for processing that information and document it.

Safeguarding

Zems Academy actively works to safeguard children, young people and vulnerable adults from harm. Zems Academy has a duty to tell Social Services where an individual's safety is at risk and share information with them, whether reported directly or indirectly to staff. The types of information that may be shared include names, contact details, information about a person's physical or mental health and relations with others.

Zems Academy has detailed procedures that cover the reporting of this information which follow various local safeguarding information sharing protocols. Zems Academy expects its staff to immediately report any concerns to the safeguarding lead who will report the information in accordance with the Safeguarding policy.

In certain limited circumstances DP legislation provides for personal data, even sensitive data, to be shared without the individual knowing about it.

Opting out
Zems Academy may use personal data for direct marketing (including to business partnerships) in relation to its activities. This includes email and text, phone calls and direct mailshots. Consent will be obtained at the time that personal data is provided by the individual. Any individual can exercise their right, at any time, to opt out of their personal data being used in this way and Zems Academy will accord with their request.

Withdrawing consent
Zems Academy acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where Zems Academy has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn

Employee training & Acceptance of responsibilities

Induction
All employees who have access to any kind of personal data will have their responsibilities outlined during their induction procedures. This will be recorded on the induction checklist and stored in their employee files.

Continuing training
Continual training will be provided for existing employees using a range of methods including online and blended learning courses, discussion during team meetings, employee correspondence and supervision from direct line managers.

Procedure for staff signifying acceptance of policy
Compliance with data protection and other relevant policies will be include in the annual employee review process.

Policy review

Responsibility
Company Directors have overall responsibility for ensuring that Zems Academy complies with its legal obligations.

Procedure
This policy will be reviewed in consultation with the Senior Leadership team to ensure it is relevant for all elements of Zems Academy's business operations.