Data Protection Policy

IID Architects is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations. We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work.

This policy meets the requirements of the General Data Protection Act 2018 (GDPR)

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed

Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller. In the case of IID Architects this would mean professional advisers, SAGE, NEST, Rapport3, Mailchimp
Business Purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: • Compliance with our legal, regulatory and corporate governance obligations and good practice • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • Ensuring business policies are adhered to (such as policies covering email and internet use) • Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting, credit scoring and checking • Investigating complaints • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments • Monitoring of staff conduct, disciplinary matters • Marketing our business • Improving services
Lawful Purposes	At least one of the following conditions must apply when processing personal data: • Consent – we hold clear, explicit and defined consent for the individual's data to be processed for a specific purpose • Contract – the processing is necessary to fulfil or prepare a contract for the individual • Legal obligation – we have a legal obligation to process the data

	(excluding a contract) • Vital interests – processing the data is necessary to protect a person's life or in a medical situation • Public function – processing is necessary to carry out a public function, a task of public interest or the function has a clear basis in law • Legitimate interest – the processing is necessary for our legitimate interests such as business purposes. This condition does not apply if there is good reason to protect the individual's data which overrides the legitimate interest

Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet use and we may supplement or amend the policy from time to time.

IID Architects is classified as a data controller and maintains registration with the Information Commissioners Office in order to continue lawfully processing data.

Data Protection Principles

IID Architects shall comply with the principles of data protection enumerated in the GDPR. The principles are:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- The data we hold must be kept safe and secure

Accountability and Transparency

We must ensure accountability and transparency in all our use of personal data. The Directors have overall responsibility for ensuring that the practice complies with its obligations under the GDPR.

Day-to-day responsibilities rest with the Practice Manager, the IT Manager or the Directors. The Practice Manager and IT Manager will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the practice of any changes to their personal data, such as a change of address.

Summary of Privacy/fair processing notice – please refer to full staff notice attached to this Policy

We only collect and use personal data when the law allows us to. Most commonly we process it where processing is required for our legitimate interest as a business or we need it to comply with a legal obligation. Less commonly, we may also process data where we have obtained consent to use it in a certain way.

Clients, Consultants and Suppliers
We hold personal data about clients, consultants and suppliers for the business purpose of running an architectural practice. We only retain this data for as long as it is necessary to satisfy the purpose for which has been collected. We do not share this information with anyone without consent.

Staff
We process data relating to those we employ to work at IID Architects. The purpose of processing this data is for business purposes. We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. We will not share information about staff with third parties without consent unless the law allows us to or requires us to. We are required, by law, to pass certain information about staff to specified external bodies, such as HMRC and insurers so that they are able to meet their statutory obligations.

In any case where we process sensitive personal data we will require the data subject's explicit consent unless exceptional circumstances apply or we are required to do this by law.

Please speak with the Practice Manager or the IT Manager in the first instance regarding any queries or issues.

Subject Access Requests
Staff have a right to request access to information the practice holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter or email. Requests should include name, correspondence address, contact number, email address and details about the information requested.

The practice will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of another individual
- Certain information relating to correspondence with practice solicitors or professional advisers.

Rights of Individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month.

4. Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.

- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Storage of records (including for Data Processors)

- Paper-based records are kept under lock and key when not in use
- Personal information is not taken off site
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices.
- Personnel, Sage Payroll, Finance, Project Directories and Approved Consultant Lists are kept on restricted access server drives with back up and disaster recovery protected behind a firewall.
- IID Architects Contacts and Project emails are employee password protected secured by Microsoft
- Rapport3 has a user based access policy
- Mailchimp is username and password protected
- The practice professional advisers and service providers are registered Data Controllers with the ICO.

Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

Staff Responsibilities

- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors and report anything suspicious or contradictory to this policy or our legal obligations without delay

Training

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 make it necessary.

.

Employee Privacy Notice

Data Controller – Initiatives in Design Limited trading as IID Architects

The organisation collects and processes personal data relating to its employees to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the organisation collect?

- Your name, address and contact details including email address and telephone number, date of birth and gender
- The terms and conditions of your employment
- Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation
- Information about your remuneration, including entitlement to benefits such as pensions or insurance cover
- Details of your bank account and national insurance number
- Information about your emergency contacts
- Information about your nationality and entitlement to work in the UK
- Information about your criminal record
- Details of your schedule (days of working and working hours) and attendance at work
- Details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals and the reasons for the leave
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- Assessments of your performance
- Information, if relevant, about medical or health conditions including whether or not you have a disability for which the organisation needs to make reasonable adjustments

This information may be collected in a variety of ways. For example data might be collected through CVs; obtained from your passport or other identity documents; from forms completed by you at the start of or during your employment; from correspondence with you; or through meetings or other assessments. In some cases the organisation may collect personal data about you from third parties such as former employers or criminal record checks permitted by law.

Data will be stored in a range of different places, including in your personnel file, in the finance folders and in other IT systems used by the organisation.

Why does the organisation process personal data?

The organisation needs to process data to enter into an employment contract with you and meet its obligations under that **employment contract** - for example to pay you and administer pension and insurance entitlements.

In some cases the organisation needs to process data to ensure it is complying with its **legal obligations** – for example to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases the organisation has a **legitimate interest** in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- Run recruitment and promotion processes
- Maintain accurate and up-to-date employment records and contact details including details of who to contact in the event of an emergency and records of employee contractual and statutory rights
- Operate and keep a record of disciplinary and grievance processes to ensure acceptable conduct within the workplace
- Operate and keep a record of employee performance and related processes such as training to plan for career development, succession planning and workforce management purposes
- Operate and keep a record of absence and absence management procedures to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled
- Obtain occupational health advice, to ensure it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay and other benefits to which they are entitled
- Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave) to allow effective workforce management, to ensure that the organisation complies with its duties in relation to leave entitlement and to ensure that employees are receiving the pay or other benefits to which they are entitled
- Ensure effective general HR and business administration
- Provide references on request for current or former employees and
- Respond to and defend against any legal claims

Who has access to data?

Your information may be shared internally, including with members of the HR/admin team including payroll, Directors and Associates and IT staff if access to data is necessary for the performance of their roles.

The organisation shares your data with third parties in order to obtain references, background checks and criminal record checks from the Disclosure and Barring Service. The organisation also shares your data with third parties that process data on its behalf such as accountants, bankers, insurers and brokers, pension providers, payroll support and IT support.

How does the organisation protect data?

The organisation takes protection of your data seriously. There are internal policies and controls in place to ensure your data is not lost, accidentally destroyed, misused or disclosed and is not accessed except by employees in performance of their duties. Where the organisation engages third parties to process personal data on its behalf, they are obliged to implement appropriate technical and organisation measures to ensure the security of data.

For how long does the organisation keep your data?

The organisation will hold your personal data for the duration of your employment and thereafter for a period of six years in archive storage.

Your rights

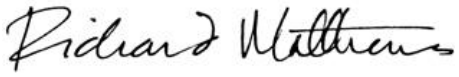
As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request
- Require the organisation to change incorrect or incomplete data
- Require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing
- Object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing if you consider your rights take precedence
- You can complain to the Information Commission if you believe the organisation has not complied with your data protection rights

What if you do not provide personal data?

You have some obligations under your employment contract to provide the organisation with data. In particular you are obliged to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data to exercise your statutory rights, such as in relation to statutory leave entitlements. Failure to provide the data may mean you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.



Richard Matthews
Director
08/05/18

Distribution:

IID Architects		