JOHNWORTH
SHOPFITTERS LTD

John Worth Shopfitters Ltd (JWS) GDPR policy

Approved by: **The Board** **Date: 23 May 2018**

Next review due by: **23 May 2021**

Purpose of the policy

JWS needs to gather and use certain information about individuals.

This will include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law. Specifically the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

Policy statement and legislation

JWS is committed to complying with both the law and good practise. We fully respect the rights of individuals and will be open and transparent with those whose data we hold/process. We are committed to ensuring information is secure, accurate and relevant.

JWS employees have been trained on GDPR to ensure compliance.

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

Types of Data

We process necessary and proportionate personal and sensitive data in relation to our duties as employers. For more detail, please see the Employee Privacy policy.

We process necessary personal data in relation to our clients, for more detail please see the Client Privacy policy.

To carry our services, we may be required to share DBS certificate number and expiry date and photographic identification images of our employees to customers who require this data for safeguarding purposes.

Where we subcontract work to other organisations, we may be required to process and share personal and sensitive data of their employees for safeguarding purposes – including DBS certification and identification images.

Occasionally we have work sub contracted to us, we will be required to share personal and sensitive data of our employees. Whenever, we permit a third party to access personal information, we will implement appropriate measures to ensure the data is used in a manner consistent with this notice and that the security and confidentiality of the data is maintained.

We operate a CCTV at our head office to prevent crime on our premises. We have notified our employees of our operating CCTV, our CCTV policy is included within our staff handbook. Our premises have prominent signage, notifying all visitors of our CCTV and we are registered with the ICO accordingly. We will adhere to the ICO's code of practice for the use of CCTV.

To enable us to manage a safe and effective fire procedure and to manage employee's hours, we collect electronic clocking in data from employees and all visitors are required to sign our visitor register.

JWS does not engage in any form of direct marketing.

Legal basis for processing data

We only process data where it meets the criteria set out in article 6 of the GDPR.

In most cases our legal basis for collecting and using the personal data will depend on the personal data concerned and the way we collect it. We will normally collect personal data where we need it to perform a contract (e.g. to manage the employer/employee relationship), where we have freely given consent to do so, or where the processing is in our legitimate interests and only where this interest is not overridden by the individual's own interests or fundamental rights and freedoms. In some cases, we may also have a legal obligation to collect personal information or may otherwise need the personal information to protect the vital interests of an individual.

Any processing based on consent will be made clear to you at the time of collection or use – consent can be withdrawn at any time by contacting the DPO.

We may also collect and use personal information when it is necessary for other legitimate purposes, such as to help us conduct our business more effectively and efficiently – for example, for general IT security management, accounting purposes or financial planning. We may also process your personal information to investigate violations of law or breaches of our own internal policies.

We collect personal data on our clients, mainly restricted to employees names and business contact details to allow us to fulfil our contractual obligations to them.

We collect employee clocking in data and visitor signing in book. We need this for two purposes. Firstly, to comply with our legal obligations to operate a fire safety procedure. Secondly, for our legitimate interests, allowing us to confirm who was on site which we may need to check if a query arises relating to a contract or payroll.

Risks

JWS's GDPR is designed to mitigate as much as is reasonable possible against the risk of data getting into the wrong hands, or by individuals being harmed because of the data being inaccurate or insufficient.

Roles and responsibilities

This policy applies to **employees**, and to external organisations or contractors working on our behalf. Employees who do not comply with this policy may face disciplinary action.

Board

The board has overall responsibility for ensuring that JWS complies with all relevant data protection obligations.

Data protection officer

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

They will where relevant, report to the board their advice and recommendations on data protection issues.

The DPO is also the first point of contact for the ICO and any data access requests and will approve all unusual or controversial disclosures of personal data.

All Third party sharing agreements will be approved by the DPO.

Our DPO is can be contacted by writing to:

Data Protection Officer, Highfields Farm Enterprise Centre, Huncote Rd, Stoney Stanton LE9 4DJ

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing JWS 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
    - 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

Collecting personal data

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Employees must only process personal data where it is necessary to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. See the retention section below.

Sharing personal data

We take care to allow access to personal data only to those who require such access to perform their tasks and duties, and to third parties who have a legitimate purpose for accessing it. Whenever we permit a third party to access personal information, we will implement appropriate measures to ensure the data is used in a manner consistent with this notice and that the security and confidentiality of the data is maintained.

We share employees and contractor's names, business contact details, photographic identification and DBS certification to organisations to who we deliver services who require this documentation in some incidences for safeguarding purposes.

In addition, we make certain personal data available to third parties who provide services to us. We do so on a "need to know basis" and in accordance with applicable data protection and data privacy laws.

For example, some personal data will be available to our employee benefit plans service providers and third-party companies who provide us with employment law advice, IT support, health and safety support, payroll support services, expenses, tax and travel management services.

We may also disclose personal data to third parties on other lawful grounds, including:

- To comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process
- In response to lawful requests by public authorities (including for national security or law enforcement purposes)
- As necessary to establish, exercise or defend against potential, threatened or actual litigation
- Where necessary to protect the vital interests of our employees or another person
- In connection with the sale, assignment or other transfer of all or part of our business; or
- With your freely given and explicit consent

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law. We will minimise the personal data to the employees' name and business contact details.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information. 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
- The source of the data, if not the individual

Subject access requests must be submitted in writing, either by letter, email to the DPO. They should include:

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

If an employee receives a subject access request they must immediately forward it to the DPO.

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
- 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 will not disclose information if it may cause serious harm to the physical or mental health of another individual.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.
A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.
When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition, 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Prevent processing that is likely to cause damage or distress
- 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 an employee receives such a request, they must immediately forward it to the DPO.

Website and Social media

We do market our services on our website and on social media - we may take recommendations, photographs and record images of individuals for that purpose.

We will obtain consent from those individuals beforehand and will clearly explain how the recommendations/ image/video will be used.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the recommendation/photograph/video and not distribute it further.

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

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.

In particular:

- Servers are kept on one site, in a secure building.
- Servers are encrypted
- Keys to the head office is restricted to company officers who require it to carry out their duties.
- Portable electronic devices, such as laptops and hard drives that contain personal data are kept locked when not in use.
- Employees are required to lock their screens when away from their desk, in addition we operate a timed-out screen saver.
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops, mobiles and other electronic devices. Passwords are changed every 3 months.
- Our IT systems are protected by up to date antivirus and Malware software
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Our email system uses Encryption software
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected
- All sites have a nominated employee with a company mobile phone, employees agree to manage the site phone and can refuse at ay time. Policy is included in the employee handbook
- Employee personal and sensitive information where practical is provided in written or electronic form to ensure accuracy.
- All paper copies of data are kept on the premises and are locked when not in use.
- Papers containing confidential personal data must not be left anywhere where there is general access
- We have a business continuity procedure in the case of emergency.

Retention policy

Personal data will be stored in accordance with applicable laws and kept for as long as needed to carry out the purposes described in this notice or as otherwise required by law.

For Employees and contractors, data specific to their employment and or training is generally retained until the end or their employment, employment application, or work relationship with us plus a reasonable period of time thereafter to respond to employment or work-related inquiries or to deal with any legal matters (e.g. judicial or disciplinary actions), document the proper termination of your employment or work relationship (e.g. to tax authorities), or to provide you with ongoing pensions or other benefits.

Successful employment applications will form part of the ongoing employee record. Unsuccessful applications will be retained no longer than 6 months.

CCTV will be retained for a minimum of 6 months and a maximum of 9 months.

All Health and safety assessments, site information and work projects are retained for a minimum of 6 years, and longer if any queries arise regarding the job.

All financial accounts which may include personal data is held for a minimum of 6 years, in according with the HMRC rules.

Data that we share with third parties on behalf of our employees such as pension providers will be retained by the Third party after employee's employment and will be retained by JWS as long as JWS has an obligation to the individual (ongoing pension or other benefits) or as long as is required by law.

Electronic clocking in data records are retained for 6 years and our visitor book is kept for the life of the book.

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

We 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.

Training

All employees who receive or process data receive 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 the companies' processes make it necessary.
https://ico.org.uk/for-organisations/resources-and-support/training-videos/

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our practice. Otherwise, or from then on, this policy will be reviewed **every 3 years** and shared with the full governing board.

19. Links with other policies

This data protection policy is linked to our employee handbook, client privacy policy and employee privacy policy.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the employee or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, 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
- The DPO will alert the board
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant employees or data processors where necessary. (Actions relevant to specific data types are set out 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
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored within the GDPR file on the Directors network
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. 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. 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - 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 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 stored within the GDPR folder on the Directors network
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, 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.

To set out the relevant actions we will take for different types of risky or sensitive personal data processed by the school. For example:

Sensitive information being disclosed via email (including safeguarding records)

- 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
- Employees who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will 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 ensure we receive 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

Appendix 2: Data protection principles

The GDPR is based on data protection principles which we 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

Appendix 3: Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username 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 an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
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.