DATA PROTECTION POLICY & PROCEDURES

Prepared By:	Emma Chilton / Ian Stephen	Date Adopted:	May 2018
Job Title:	Head of HR / Head of Finance	Status:	Recommended
Authorised By:	Kate Grant	Last Reviewed:	September 2021
Job Title:	CEO	Ratified:	October 2021
Reviewed by:	Emma Chilton	Next Review date:	January 2022
Job Title:	Director of People	Version:	3.1

jigsaw trust
INSPIRED BY AUTISM

TABLE OF CONTENTS

1. Purpose

1.1 The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

1.2 Jigsaw Trust will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils/learners, parents, suppliers, employees, workers and other third parties.

2. Definitions

2.1 **Jigsaw Trust / The Trust** includes Jigsaw CABAS® School, Jigsaw Plus and Jigsaw Trading 2013 Limited (Café on the Park);

2.2 **Personal data** - Any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

2.2.1 Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

2.2.2 Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

2.3 **Special Category Data -** Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

2.4 **Data processing** - Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

2.5 **Data Subject'** - An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

2.6 **Data Controller** - The natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of processing the personal data;

2.7 **Data Processor** - A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

2.8 **Recipient** - A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;

2.9 **Consent of the data subject** - Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

2.10 **Parental Consent** - The consent of a guardian, advocate or deputy;

2.11 **Personal data breach** - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

2.12 **Third party** - A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

2.13 **Third country** - Any country recognised as not having an adequate level of legal protection for the rights of freedoms of data subjects in relation to processing personal data;

2.14 **Data Protection Authority** - An independent Public Authority responsible for monitoring the application of the relevant Data Protection legislation;

2.15 **Restriction of processing -** 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

2.16 **Encryption -** The process of converting information or data into code, to prevent unauthorised access;

2.17 **Pseudonymisation** The processing of personal data in such a manner that the personal daa can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

2.18 **Data Protection Impact Assessment (DPIA)** - DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

2.19 **Criminal Records Information** - Personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

3. Scope

3.1 This policy applies to:

- Jigsaw Trust, including Jigsaw CABAS School, Jigsaw Plus, and Jigsaw Trading 2013 Limited (Café on the Park);
- All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

- All volunteers, contractors, suppliers and other people working on behalf of Jigsaw Trust

3.2 This policy does not form part of any individual's terms and conditions of employment with The Trust and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

4. Data Protection Principles

4.1 Jigsaw Trust is responsible for and adheres to the principles relating to the processing of personal data as set out in the UK GDPR.

4.2 The principles the Trust must adhere to are set out below.

4.3 Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

4.3.1 The Trust only collects, processes and shares personal data fairly and lawfully and for specified purposes. The Trust must have a specified purpose for processing personal data and special category of data as set out in the UK GDPR.

4.3.2 Before the processing starts for the first time the Trust will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to 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).

4.4 Personal Data

4.4.1 The Trust may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the Trust's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

4.5 Special Category Data

4.5.1 The Trust may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Trust in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing in necessary for archiving, statistical or research purposes.

4.5.2 The Trust identifies and documents the legal grounds being relied upon for each processing activity.

4.6 Consent

4.6.1 Where the Trust relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

4.6.2 Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

4.6.3 A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

4.6.4 Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

4.6.5 If explicit consent is required, the Trust will normally seek another legal basis to process that data. However if explicit consent is require the data subject will be provided with full information in order to provide explicit consent.

4.6.6 The Trust will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

4.7 Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

4.7.1 Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

4.7.2 The Trust will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

4.8 Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

4.8.1 The Trust will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

4.8.2 When personal data is no longer needed for specified purposes, the Trust shall delete or anonymise the data.

4.9 Principle 4: Personal data must be accurate and, where necessary, kept up to date

4.9.1 The Trust will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

4.9.2 Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Trust.

4.10 Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

4.10.1 Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Trust will ensure that they adhere to legal timeframes for retaining data.

4.10.2 We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

4.11 Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

4.11.1 In order to assure the protection of all data being processed, the Trust will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -

- Encryption;

- Pseudonymisation
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

4.11.2 The Trust follows procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

4.11.3 The Trust will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

4.11.4 Full details on the Trust's security measures are set out in the Trust's IT Security Policy.

4.12 Sharing Personal Data

4.12.1 The Trust will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

- Has a need to know the information for the purposes of providing the contracted services;
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

4.12.2 There may be circumstances where the Trust is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

4.12.3 The intention to share data relating to individuals to an organisation outside of our Trust shall be clearly defined within written notifications and details and basis for sharing that data given.

4.13 Transfer of Data Outside the European Economic Area (EEA)

4.13.1 The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

4.13.2 The Trust will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the Trust's guidelines on transferring data outside of the EEA. For the

avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

4.14 Transfer of Data Outside the UK

4.14.1 The Trust may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, standard data protection clauses or compliance with an approved code of conduct**.**

5. Data Subject Rights and Requests

5.1 Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

5.2 The rights data subjects have in relation to how the Trust handles their personal data are set out below: -

(a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;

(b) Receive certain information about the Trust's processing activities;

(c) Request access to their personal data that we hold (see Subject Access Request section below)

(d) Prevent our use of their personal data for marketing purposes;

(e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(f) Restrict processing in specific circumstances;

(g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) Request a copy of an agreement under which personal data is transferred outside of the EEA;

(i) Object to decisions based solely on automated processing;

(j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

(k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(l) Make a complaint to the supervisory authority; and

(m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

5.3 If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the Trust to verify the identity of the individual making the request.

5.4 Subject Access Requests

5.4.1 An individual has the right, subject to certain exemptions, to access the personal information that an organisation holds about them. Accessing personal data in this way is known as making a Subject Access Request or SAR (Refer to the Subject Access Request Policy for more information).

5.4.2 Anyone wishing to make a request under any of the above rights, can do so by contacting Jigsaw's Data Protection Team on dataprotection@jigsawtrust.co.uk. Jigsaw Trust will confirm the receipt of the request in writing. A response to each request will normally be provided within 30 days.

5.4.3 Jigsaw Trust will carry out appropriate verification checks to confirm the identity of the requestor and that the requestor is the data subject.

5.4.4 Jigsaw Trust will keep a log of all requests. Any member of staff, who receives a subject access request, must inform Jigsaw's Data Protection Team on dataprotection@jigsawtrust.co.uk without delay.

5.5 Direct Marketing

5.5.1 The Trust is subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

5.5.2 The Trust will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Trust will promptly respond to any individual objection to direct marketing.

5.6 Employee Obligations

5.6.1 Employees may have access to the personal data of other members of staff, suppliers, parents or pupils/learners of the Trust in the course of their employment or engagement. If so, the Trust expects those employees to help meet the Trust's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction. Please refer to the Trust's IT Security Policy for further details about our security processes);
- Not to remove personal data or devices containing personal data from the Trust premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;
- Not to store personal information on local drives.

6. Accountability

6.1 The Trust will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

6.2 The Trust has taken the following steps to ensure and document UK GDPR compliance:

6.3 Jigsaw Trust has a designated person responsible for data protection, known as the Data Protection Officer (DPO). The Data Protection Officer is responsible for overseeing data protection within the school so if you do have any questions in this regard, please do contact them on the information below:

Data Protection Officer: Judicium Consulting Limited

Address: 72 Cannon Street, London, EC4N 6AE

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0203 326 9174

Lead Contact: Craig Stilwell

6.4 The DPO should be contacted with any questions about the operation of this Data Protection Policy or the UK GDPR or if where there are concerns that this policy is not being or has not been followed. In particular, the DPO should be contacted in the following circumstances: -

(a) If you are unsure of the lawful basis being relied on by the Trust to process personal data;

(b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);

(c) If you need to draft privacy notices or fair processing notices;

(d) If you are unsure about the retention periods for the personal data being processed after reference to the Trust's data retention policy;

(e) If you are unsure about what security measures need to be put in place to protect personal data;

(f) If there has been a personal data breach, after reference to the procedure set out in the Trust's breach notification policy;

(g) If you are unsure on what basis to transfer personal data outside the EEA;

(h) If you need any assistance dealing with any rights invoked by a data subject;

(i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

(j) If you plan to undertake any activities involving automated processing or automated decision making;

(k) If you need help complying with applicable law when carrying out direct marketing activities;

(l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

6.5 Personal Data Breaches

6.5.1 The UK GDPR requires the School to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

6.5.2 We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

6.5.3 If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Jigsaw Data Protection Team, dataprotection@jigsawtrust.co.uk, who is the key point of contact for personal data breaches or your DPO.

6.6 Transparency and Privacy Notices

6.6.1 The Trust will provide detailed, specific information to data subjects. This information will be provided through the Trust's privacy notices, which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them.

6.6.2 Privacy notices sets out information for data subjects about how the Trust uses their data and the Trust's privacy notices are tailored to suit the data subject.

6.6.3 Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR including the identity of the data protection officer, the Trust's contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notice.

6.6.4 When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The Trust will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

6.6.5 Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the UK GDPR

6.7 Privacy By Design

6.7.1 The Trust adopts a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

6.7.2 Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the Trust takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

6.8 Data Protection Impact Assessments (DPIAs)

6.8.1 In order to achieve a privacy by design approach, the Trust conducts DPIAs for any new technologies or programmes being used by the Trust which could affect the processing of personal data. In any event the Trust carries out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data;
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

6.8.2 Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

6.9 Records & Confidentiality

6.9.1 Jigsaw Trust will keep a record of processing activities under its responsibility. That record is kept as an electronic data audit and contains all of the following information:

- contact details for Jigsaw Trust as the controller and processor, any joint controllers and the person responsible for data protection within Jigsaw Trust;
- the purposes of processing;
- the categories of processing carried out on behalf of Jigsaw Trust description of categories of the data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
- time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures applied by Jigsaw Trust.

6.9.2 Jigsaw Trust will also keep records on staff training linked to data protection, subject access requests and retention procedures for personal data. These records will be kept in an electronic format as part of Jigsaw Trust's central data protection compliance record.

6.10 Data Storage and Security

6.10.1 Jigsaw Trust will ensure that personal data are kept securely by implementing appropriate technical and operational measures.

6.10.2 To ensure security of personal data on paper Jigsaw Trust will make all reasonable efforts to:

- keep personal data in locked cabinets, drawers when not required;
- follow a 'clear desk' policy;
- ensure printouts with personal information are not left on printers;
- shred and securely dispose of any documents, printouts once they are no longer required.

6.10.3 Where data are stored electronically, Jigsaw Trust will ensure that personal information is protected from unauthorised access, accidental deletion and malicious hacking attempts by:

- keeping servers in a secure location away from general office space
- protecting servers by appropriate security software and a firewall;
- backing up data at least daily;
- testing of back-up procedures and security of systems are undertaken from time to time;
- use of strong passwords. Passwords should never be shared between employees;
- using password protection for accessing ICT devices;
- locking screens on devices when devices are unattended.
- storing data on designated Jigsaw Trust drives and servers. Employees should not store data on their C drives as this is not backed up
- encrypting hard drives and USB devices;
- encrypting personal data when it is transferred from Jigsaw Trust to a third party;
- not saving or downloading personal data directly to laptops, mobile devices (e.g. tablets, smartphones), desktops.

6.10.4 For more information on Jigsaw Trust's measures on ICT security, refer to ICT Security Policy and Procedures.

6.11 Training

6.11.1 The Trust will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

6.12 Audit

6.12.1 The Trust, through its Data Protection Officer regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

7. Complaints

7.1 Complaints will be dealt with in accordance with Jigsaw Trust Complaints Policies. Complaints relating to the handling of personal data may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or at www.ico.gov.uk.

8. Contacts

8.1 Any enquiries in relation to this policy should be directed to Clerk to the Trustees and Governors (Clerk to Trustees and Governors) clerk@jigsawtrust.co.uk.

9. Roles and responsibilities

9.1 Everyone who works for or with Jigsaw Trust has some responsibility for ensuring data is collected, stored and handled appropriately and securely. Each team that handles personal data must ensure that it is handled and processed in line with this policy and procedures and data protection principles.

9.2 Board of Trustees and CEO are responsible for:

- ensuring that Jigsaw Trust complies with data protection law and regulation;
- implementing appropriate policies and procedures;
- ensuring privacy notices are accessible to data subjects;
- having a data protection officer in place.

9.3 Data Protection Officer is responsible for:

- keeping the board of trustees and school governors updated about data protection responsibilities, risks and issues;
- reviewing all data protection procedures and related policies, in line with an agreed schedule;
- arranging and providing data protection training and advice for the people covered by this policy;
- responding to data protection questions from staff and anyone else covered by this policy;
- dealing with requests from individuals to see the data Jigsaw Trust holds about them (also called 'Subject Access Requests');
- informing ICO of any personal data breach and acting as point of contact until the matter is resolved;

- checking and approving any contracts or agreements with third parties that may handle the company's sensitive data;
- keeping up to date records on processing activities and training within the organisation.

9.4 IT Lead is responsible for:

- ensuring all systems, services and equipment used for storing data meet acceptable security standards;
- performing regular checks, tests and scans to ensure security hardware and software is functioning properly;
- evaluating any third-party services that the company is considering using to store or process data. For instance, cloud computing services.

9.5 All staff are responsible for:

- complying with this policy and integrated procedures;
- keeping personal information and other records accurate and up to date;
- using and keeping personal data securely;
- deleting personal information that is no longer required in line with retention schedules;
- informing the data protection officer of any requests of access to personal data;
- informing the data protection officer of any data protection issues, personal data breaches.

10. Policy Review

10.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. The policy review will be undertaken by the person responsible for data protection alongside other appropriate staff within Jigsaw Trust.

10.2 This policy was last reviewed in September 2021.

11. Version History

No.	Date	Amendment
1.1	May 2018	Original
1.2	Sep 2018	Privacy Notice added as Appendix 1
1.3	Oct 2018	Retention Schedule added as Appendix 2
2.1	Jan 2020	Updated to reflect current procedure
2.2	June 2021	Policy review: terminology and scope updated.
2.3	June 2021	Amended Privacy notice in line with current version.
2.4	June 2021	Updated DPO to Judicium
3.1	August 2021	Comprehensive review of policy to update and incorporate recommendations from Judicium's policy template

12. Related Legislation & Guidance

Document	Location
Data Protection Act 2018	http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
General Data Protection Regulation (GDPR)	https://gdpr-info.eu
UK GDPR Guidance	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

13. Related Internal Documentation

Document	Electronic Copy Location
IT Security Policy	Common / MyJigsaw / POLICIES / Jigsaw Trust / GDPR
IT Acceptable Use Policy	Common / MyJigsaw / POLICIES / Jigsaw Trust / GDPR
Data Breach Policy	Common / MyJigsaw / POLICIES / Jigsaw Trust / GDPR
Subject Access Request (SAR) Policy	Common / MyJigsaw / POLICIES / Jigsaw Trust / GDPR
CCTV Policy	Common / MyJigsaw / POLICIES / Jigsaw Trust / GDPR
Mobile Devices Policy	Common / MyJigsaw / POLICIES / Jigsaw Trust / GDPR
Password Policy	Common / MyJigsaw / POLICIES / Jigsaw Trust / GDPR
Records Management and Retention Procedures	Operations / 111 GDPR