DATA BREACH POLICY

Prepared By:	Kate Grant	Date Adopted:	July 2018
Job Title:	CEO	Status:	Recommended
Authorised By:	Kate Grant	Last Reviewed:	November 2023
Job Title:	CEO	Ratified:	December 2023
Reviewed by:	Emma Chilton	Next Review date:	November 2025
Job Title:	Director of People	Version:	2.2

TABLE OF CONTENTS

1. Purpose

1.1 The UK General Data Protection Regulation (UK GDPR) 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. The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below.

1.2 Whilst Jigsaw, as a UK organisation is subject to UK GDPR, Jigsaw could also be subject to EU GDPR if it handles the data of EU persons (which include EU clients and investors) as per EU GDPR Article 3(2)[1]. Hence forth, unless otherwise stated all references GDPR are to both UK and EU GDPR ('GDPR').

1.3 This policy relates to all personal and special categories (sensitive) data held by Jigsaw regardless of format.

1.4 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.5 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, a detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2. Definitions

2.1 'Jigsaw' 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.

2.3 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.

2.4 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.

2.5 **Special Category Data** - Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual'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.

2.6 **Personal Data Breach** - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

[1] EU GDPR Article 3(2): "This Regulation applies to the processing of personal data of data subjects who are in the Union **by a controller or processor not established in the Union**, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union…"

2.7 Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (for example sending an email or SMS to the wrong recipient)
- Unforeseen circumstances such as a fire or flood
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it

2.8 This list is non-exhaustive and for the purpose of this policy, data security breaches include both confirmed and suspected incidents.

2.9 **Data Subject** - Person to whom the personal data relates.

2.10 **ICO** - Information Commissioner's Office, the UK's independent regulator for data protection and information.

2.11 **DPO** is an acronym for Data Protection Officer

2.12 **LIO** is an acronym for Lead Investigating Officer

3. Scope

3.1 The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

3.2 This policy applies to all staff at Jigsaw. This includes temporary, casual or agency staff and contractors, consultants, suppliers, and data processors working for, or on behalf of Jigsaw. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it.

3.3 Training will be provided to all staff to enable them to carry out their obligations within this policy.

3.4 Data Processors will be provided with a copy of this policy and will be required to notify Jigsaw of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

3.5 Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under Jigsaw's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

3.6 This policy does not form part of any individual's terms and conditions of employment with Jigsaw 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. Reporting a data breach

4.1 Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time, and we would encourage all staff to report any concerns (even if they do not meet the criteria of a data breach) to Jigsaw's Data Protection Team – dataprotection@jigsawtrust.co.uk or the DPO. This can help capture risks as they emerge, protect Jigsaw from data breaches and keep our processes up to date and effective.

4.2 Any individual who suspects a personal data breach has occurred, may have occurred, or may occur, should: -

- Complete a Data Breach Report Form (which can be found in the GDPR folder on the School, JigsawPlus or TSS Homepages and a copy of which is provided at Appendix 1);
- Email the completed form to Jigsaw's Data Protection Team dataprotection@jigsawtrust.co.uk copying the IT Helpdesk ict@jigsawtrust.co.uk if applicable.

4.3 Where appropriate, the reporting individual should liaise with their line manager about completion of the Data Breach Report Form. Breach reporting is encouraged throughout Jigsaw and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, the Data Protection Team (email dataprotection@jigsawtrust.co.uk) or the DPO.

4.4 Once reported, the reporting individual should not take any further action in relation to the breach. In particular s/he must not notify any affected individuals or regulators or investigate further. The Data Protection Team will acknowledge receipt of the Data Breach Report Form and take appropriate steps to deal with the report in collaboration with the DPO.

4.5 The Data Protection Officer is responsible for overseeing data protection within Jigsaw, 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

4.6 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The requirement to report a breach to the ICO within 72 hours of becoming aware of it applies even if the breach is discovered outside of normal business hours.

I4.7 The report must include full and accurate details of the incident, including the date and time the breach was discovered; when the breach occurred (dates and times); who is reporting it; a description of the breach; what personal data was involved; how many individuals are involved; what the consequences of the breach were and what action was taken to mitigate it.

5. Managing and Recording the Breach

5.1 On being notified of a suspected personal data breach, The Data Protection Team will notify the DPO as needed. Collectively they will take immediate steps to establish whether a personal

data breach has in fact occurred. If so, they will take steps to:

- Where possible, contain the data breach
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed
- Assess and record the breach in Jigsaw's data breach register
- Notify the ICO where required
- Notify data subjects affected by the breach if required
- Notify other appropriate parties to the breach
- Take steps to prevent future breaches

5.2 The investigation will need to take into account the following:

- the type of data involved
- its sensitivity
- the protections are in place (e.g. encryptions)
- what impact the data loss could have (e.g. what has happened to the data; whether the data could be put to any illegal or inappropriate use)
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach.

6. Notifying the ICO

6.1 The DPO will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

6.2 This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (I.e. it is not 72 working hours). If Jigsaw is unsure of whether to report a breach, the assumption will be to report it.

6.3 Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

7. Notifying Data Subjects

7.1 Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, The Data Protection Team will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures Jigsaw has (or intends) to take to address the breach.

7.2 When determining whether it is necessary to notify individuals directly of the breach, The Data Protection Team will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

7.3 If it would involve disproportionate effort to notify the data subjects directly (for example, by

not having contact details of the affected individual) then Jigsaw will consider alternative means to make those affected aware (for example by making a statement on Jigsaw's website).

8. Notifying Other Authorities

8.1 Jigsaw will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers
- Parents
- Third parties (for example when they are also affected by the breach)
- Local authority
- The police (for example if the breach involved theft of equipment or data)

8.2 The LIO and or the DPO will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

8.3 A record will be kept of any personal data breach, regardless of whether notification was required.

9. Assessing the Breach

9.1 Once the initial incident is contained, the Data Protection Team will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

9.2 Jigsaw will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether it is necessary to conduct a privacy or data protection impact assessment
- Consider whether further audits or data protection steps need to be taken
- To update the data breach register
- To debrief trustees/governors/management following the investigation.

9.3 The Data Protection Team will, with support of relevant staff, agree and implement preventative measures (e.g. changes to systems, policies and procedures, and/or measures to increase staff awareness).

9.4 The DPO will be responsible for ensuring that remedial measures taken are effective.

10. Policy Review

10.1 We will monitor the effectiveness of this and all our policies and procedures and conduct a full

review and update as appropriate.

10.2 Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to Jigsaw.

10.3 This policy was last reviewed in November 2023.

11. Version History

No.	Date	Amendment
1.2	August 2019	Removal of flowchart
1.3	Jan 2020	Updated Data Breach form. Clarified process of data breach reporting in section 4
1.4	October 2020	Section 5.4 removal of requirement for LIO to notify police, as this is covered at 6.4 Section 2.6 Definition for LIO added in
1.5	June 21	Addition at 4.2 of DPO as Judicium
2.1	October 21	Comprehensive review to incorporate information held within Judicium's Data Breach Policy template
2.2	November 2023	Policy Review: Updated Data Breach Reporting Form provided in Appendix 1. Update at 1.2 with footnote. No other material changes

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), 2018	https://gdpr-info.eu

13. Related Internal Documentation

Document	Electronic Copy Location
Data Protection Policy	Common / MyJigsaw / Policies / Trust / GDPR
IT Security Policy	Common / MyJigsaw / Policies / Trust / IT
IT Acceptable Use Policy	Common / MyJigsaw / Policies / Trust / IT
Mobile Devices Policy	Common / MyJigsaw / Policies / Trust / IT
Subject Access Request Policy	Common / MyJigsaw / Policies / Trust / GDPR
Records Management and Retention Procedures	Operations / GDPR

APPENDIX 1 - Data Breach Report Form

Remember that in cases of a serious data breach, the ICO must be informed within 72 hours of the breach being discovered. Therefore, please act quickly to support this process

If you discover a data breach or a suspected breach, please complete Section 1 of this form and email as follows:

- **School staff** send to Emma Hawkins (emmahawkins@jigsawschool.co.uk) and Mariann Szabo (mariannszabo@jigsawschool.co.uk), cc Jigsaw's Data Protection Team on dataprotection@jigsawtrust.co.uk and Jigsaw's IT Team help@jigsawtrust.on.spiceworks.com (if necessary)
- **JigsawPlus staff** send to David Goff / Simon Wright, Jigsaw's Data Protection Team on dataprotection@jigsawtrust.co.uk and Jigsaw's IT Team help@jigsawtrust.on.spiceworks.com (if necessary)
- **TSS staff** send to your line manager, Jigsaw's Data Protection Team on dataprotection@jigsawtrust.co.uk and Jigsaw's IT Team help@jigsawtrust.on.spiceworks.com (if necessary)

This form can be found at file://js02/common/My%20Jigsaw/GDPR/

Section 1: Notification of a data breach

Please do not put the names of the people who are affected by the breach within the form. For example, refer to them as "staff member" or "pupil A" or "6 pupils were affected" rather than referring to them by name.

Name of person reporting breach: (Full name, job role and team / function if a member of staff)
Contact details of person reporting breach: (Full name, job role and team / function if a member of staff, email address, telephone number)
When did the breach happen? (DD-MM-YYYY and time if known)
When did you discover the breach? (DD-MM-YYYY and time if known)

Please describe what happened (Tell us as much as you can about the nature of the breach)
Please describe how the incident occurred (Details of how the breach happened including any series of events which have led to the breach. If some details are outstanding, explain why here (for example still investigating the breach effects)).
How did you find out about the breach? (For example was it reported by a parent or staff member)
What preventive measures were in place? (For example limited access to the information, encryption of email)
Was the breach caused by a cyber incident? For example hacking or malware – please indicate Yes No Don't know

Section 2: Assessing the severity

Section to be completed by a member of senior management, in conjunction with the Head of area affected by the breach and the IT Team where applicable.

Number of personal data records concerned? (This could be the same as data subjects affected below. If not yet known explain why)
How many data subjects could be affected? (That is those whose data has been breached rather than who received the data incorrectly
Categories of personal data included in the breach (highlight all that apply) Data revealing racial or ethnic origin Political opinions Religious or philosophical beliefs

Trade union membership
Sex life data
Sexual orientation data
Gender reassignment data
Health data
Basic personal identifies e.g name, contact details
Identification data e.g usernames, passwords
Economic and financial data e.g credit card numbers, bank details
Official documents e.g driving licences
Location data
Genetic or biometric data
Criminal convictions, offences
Not yet known
Other
Categories of data subjects affected (highlight all that apply)
Employees
Workers
Contractors
Volunteers
Pupils
Adult learners
Parents / Guardians
Previous employees, workers, contractors or volunteers
Former pupils
Former adult learners
Not yet known
Other

Potential consequences of the breach?

Please describe the possible impact on data subjects as a result of the breach. Please state if there has been any actual harm to data subjects. Detail potential risks to the individual if known. We can help complete this for you but examples include loss of data, discrimination, loss of privacy, safeguarding concerns, identity theft and lack of security on their data.

Is the personal data breach likely to result in a high risk to data subjects? (Highlight which applies) Yes No Not yet known Please give details Please detail the likelihood of harm and why the likelihood is likely/unlikely
(Cyber incidents only) Recovery time (highlight as appropriate) We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident. We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this. We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, ie backups failed, no current backup, backup encrypted etc. We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident. Other
Had the staff member involved in this breach received data protection training in the last two years? (Highlight which applies) Yes No Don't know
If there has been a delay in reporting this breach, please explain why. (Initial reports only) please give details. So only detail here if you were unable to report the breach to the ICO within the 72 hour time limit.

Section 3: Action Taken

Section to be completed by a member of senior management, in conjunction with the manager of area affected by the breach and the IT Team where applicable. Advice should also be sought from Director of People and / or CEO as needed.

Describe the actions you have taken, or propose to take, as a result of the breach.

(Describe the actions you have taken, or propose to take, as a result of the breach. Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, e.g confirmed data sent in error has been destroyed, updated passwords, planning information security training)

Have you taken actions to contain the breach? Please describe these remedial actions (For example recalling an email, sending an announcement)
Outline any steps you are taking to prevent a recurrence, and when you expect they will be completed. (For example training, policy, security measures)
Have you told data subjects about the breach? (Highlight which applies) Yes - we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects Yes - we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway No - but we are planning to because we have determined it is likely there is a high risk to data subjects No - we determined the incident did not meet the threshold for communicating it to data subjects Other
Have you told, or are you planning to tell any other organisations about the breach? (E.g. the police, other regulators or supervisory authorities. In case we need to make contact with other agencies) **(Highlight which applies)** Yes No Don't know **If you answered yes, please specify who you are informing and what you are informing them.**

Section 4: Trust information

To be completed by Kate Grant, CEO, as designed individual accountable for data protection, or her nominated deputy, prior to report being shared with Judicium as the Trust's Designated Safeguarding Officer or other authorities if required.

Organisation (data controller) name (This is the name of the School, Plus, Trust)
Registration number (This is your ICO number. You can find this on your ICO certificate or by searching ICO register of fee payers)
If not registered, please give exemption reason (Not required unless don't have ICO registration number)
Registered organisation address (School / Plus / Trust address)
Person making this report (Please provide your full name, email address and phone number in case we need to contact you about this report. If no name is put this will go only to the DPO)