**Gendered Intelligence**

**Data Protection Policy**

Contents

1. Introduction ..... 1
2. Data protection principles ..... 2
3. Individual rights ..... 2
4. Data security and breaches ..... 3
5. Photographs and other visual material ..... 3
6. Impact assessments ..... 3
7. International data transfers ..... 4
8. Data sharing ..... 4
9. Exemptions ..... 4
10. Individual responsibilities ..... 4
11. Training ..... 5
12. Document review process ..... 5

## 1. Introduction

*Purpose*

Gendered Intelligence is committed to being transparent about how it collects and uses personal data, and to meeting its data protection obligations under the General Data Protection Regulation (GDPR), which came into force on 25th May 2018. This policy sets out Gendered Intelligence's commitment to data protection, and the rights of individuals in relation to personal data.

This policy applies to the personal data of employees (including temporary employees and contractors), job applicants, former employees, Board Members, volunteers, donors, suppliers, clients and service users.

We have attempted to make this policy concise and simple to read and understand. This policy contains references to other related policies and procedures, which can be found on www.genderedintelligence.co.uk/data or by request from info@genderedintelligence.co.uk. Jay Stewart, CEO, has been appointed as the Named Representative with responsibility for data protection compliance within Gendered Intelligence. He can be contacted at jay.stewart@genderedintelligence.co.uk. Questions about any of these policies should be directed to him. Further information is also available from the Information Commissioner's Office at www.ico.org.uk.

*Definitions*

**"Data"** includes information processed on computer, or kept in paper files where there is a filing system in place to enable you to locate data about individuals.

**"Personal data"** is any information that relates to an individual who can be identified from that information.

**"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

**"Processing"** is any use that is made of data, including collecting, storing, using, amending, disclosing or destroying it.

**"Criminal offence data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

**2. Data protection principles**

Gendered Intelligence processes personal data in accordance with the six data protection principles outlined in the GDPR. GI will:

- process personal data lawfully, fairly and in a transparent manner.
- collect personal data only for specified, explicit and legitimate purposes.
- process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- keep accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- keep personal data only for the period necessary for processing.
- adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Where Gendered Intelligence processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on Special Categories of Data and Criminal Offence Data.

**3. Individual rights**

The GDPR lists eight rights that individuals have in relation to their personal data.

1. The right to be informed. GI will tell individuals what we plan to do with their data, how we will use the data, how long we will keep it and who we will share it with. This will be made clear in our Privacy Notices and Retention Policy, and we will not process personal data for any other reasons.

2-7. Data always belongs to the person, called the ‘data subject’, and not to the organisation processing it. The data subject therefore has the right to: request access to their data; rectification if data is inaccurate, or completion if incomplete; erasure of their data (also called the ‘right to be forgotten’); restriction of processing; data portability if they want to move their data to another organisation; object, for example to direct marketing.

   If you want to see your data or make any changes to how we process it, please use the Subject Access Request (SAR) Procedure.

8. Data subjects also have rights in relation to automated decision making and profiling, where decisions are made with no human involvement. GI does not undertake this or request anyone else to do this with your data.

**4. Data security and breaches**

Gendered Intelligence takes the security of personal data seriously. Gendered Intelligence has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. For more information see our Data Security Policy.

Where Gendered Intelligence engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Data breaches will always be treated seriously. Gendered Intelligence has a Data Security Breach (DSB) Procedure which outlines how it will deal with any data breach, including how and when it will communicate with data subjects.

**5. Photographs and other visual material**

Photos and videos of individuals are also personal data. Any member of staff or volunteers taking images of individuals which are intended for publication, whether internally or externally, should obtain written consent using the appropriate form, which must be stored securely once signed.

**6. Impact assessments**

Data processing may result in risks to privacy. Where an initial assessment suggests that processing would result in a high risk to individual's rights and freedoms, Gendered Intelligence will carry out a full Data Protection Impact Assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

**7. International data transfers**

Gendered Intelligence will not transfer personal data to countries outside the EEA.

**8. Data sharing**

Gendered Intelligence may be required to share certain data with other individuals or organisations. The circumstances leading to such sharing include:

- Fulfilling contractual obligations, such as payroll, pensions, or providing Statutory Sick Pay
- Meeting Health & Safety obligations, and ensuring access for disabled individuals
- Safeguarding individuals and providing information in the event of medical emergencies
- Delivering services such as events or mailing lists

We will only share the data that is strictly necessary for the purpose.

**9. Exemptions**

The following sets of information are exempt from the Data Protection Act 2018 and therefore are excluded from this policy.

- Information which Gendered Intelligence is required by law to be made public
- Information which Gendered Intelligence is required to be disclosed in connection with legal proceedings
- Information relating to national security
- Personal data processed for the prevention of crime or prosecution of offenders or for the collection of tax
- Information relating to any regulatory activity
- Information relating to special purposes which may be one or more of the following:
    - The purpose of journalism
    - Artistic purposes
    - Literary purposes

**10. Individual responsibilities**

Individuals are responsible for helping Gendered Intelligence keep their personal data up to date. Individuals should let Gendered Intelligence know if data provided to Gendered Intelligence changes, for example if an individual moves house or changes their bank details.

Individuals may have access to the personal data of other individuals, including employees, clients and service users in the course of their involvement with Gendered Intelligence. Where this is the case, Gendered Intelligence relies on individuals to help meet its data protection obligations.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside Gendered Intelligence) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from Gendered Intelligence's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Gendered Intelligence's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or service user data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Further details about Gendered Intelligence's security procedures can be found in its Data Security Policy. Gendered Intelligence reserves the right to randomly check emails, website use and telephone use in order to protect itself against unlawful use or access. Any such monitoring will be conducted in a lawful and fair manner.

**11. Training**

Gendered Intelligence will provide training to all staff, Board members and volunteers about their data protection responsibilities as part of their induction process, or as soon afterwards as is practical.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

**12. Document review process**

Gendered Intelligence will review this policy and the related policies and procedures on a bi-annual basis.

Version: 1.0
Draft approved for circulation: May 2018
Board approval due: July 2018
Review due: July 2020