Simple Data Protection Policy

Introduction and Scope

This policy explains our commitment to data protection and compliance with the UK Data Protection Act 2018. It ensures that all personal data held by Stripes is processed lawfully, fairly, and transparently, and that the rights of individuals are protected. This policy applies to everyone working for Stripes including trustees, staff, and volunteers.

Data Protection

Data protection involves safeguarding personal information by following data protection principles and the Data Protection Act 2018. The UK Information Commissioner's Office (ICO) provides guidelines that we adhere to.

- **UK GDPR:** Outlines rules for processing personal data in the UK.
- **Data Processor:** Processes personal data for a data controller.
- **Data Controller:** Decides how and why personal data is processed.
- **Data Subject:** Individual whose personal data is processed.
- **Processing:** Any operation on personal data (e.g., collection, storage, use).
- **Personal Data:** Information that can identify a living person.
- **Sensitive Personal Data:** Data needing extra protection (e.g., health information).
- **Direct Marketing:** Communication promoting a product or service to an individual.
- **PECR:** Rules for electronic direct marketing.
- **Valid Consent:** Freely given, specific, informed, and withdrawable consent.
- **Legitimate Business Purpose:** Lawful reason for processing data necessary for the interests of the data controller or a third party.

Data Protection Principles

- The UK GDPR sets out seven key principles:
    - Lawfulness, fairness and transparency – that you have a lawful basis for processing information
    - Purpose limitation – process data only for the purpose it was intended
    - Data minimisation – only collect and keep the data required
    - Accuracy – take reasonable measures to ensure the data is accurate
    - Storage limitation – only keep data as long as it is needed
    - Integrity and confidentiality (security)
    - Accountability
- These principles should lie at the heart of your approach to processing personal data.

Individual Rights

The GDPR and DPA 2018 enhances the rights of individuals in respect of their own data held by an organisation and Stripes has a legal obligation to identify that an individual has made a request under the following rights and to handle it accordingly, this includes the following rights:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related automated decision-making, including data profiling

Subject Access Request (SARs)

A SAR is when someone asks to see the personal information that WYADHD holds about them. The purpose of a SAR is to make individuals aware of and allow them to confirm the lawfulness of processing of their personal data. Under the GDPR and the current Data Protection Act (DPA), individuals have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:

- the reasons why their data is being processed;
- the description of the personal data concerning them;
- anyone who has received or will receive their personal data; and
- details of the origin of their data if it was not collected from them.
- The subject access request must be in writing (email requests are acceptable)
- The data subject's identity must be verified photographic evidence preferred– this must be documented and a copy retained
- The requester should provide sufficient information to identify the person making the request to locate the information requested
- The data subject (e.g. patient, customer) must provide enough information for the organisation to be able to process the request
- We can reconfirm with the data subject exactly which information is required (e.g. are they looking for something specific)
- The organisation reserves the right to charge if considered applicable. Under the GDPR, a request for personal information is free unless the request is 'manifestly unfounded or excessive'. Stripes could charge a 'reasonable fee' for multiple requests if appropriate.
- Subject access requests must be dealt with within 1 calendar month. This deadline can be extended by a further two months where there are a number of requests or the request is complex but you must contact the individual within a month of receipt, explaining why the extension is necessary.
- Day One starts on receipt of the request AND formal identification (photographic wherever possible)
- Once the information has been identified and collated, it must be checked by a relevant professional or line manager.
- Consider if the data subject needs to meet with a member of staff to go through the records before they are released to go through the information to ensure they understand the content and have the opportunity to have things explained to them. this maybe particular relevant if the information is of a clinical nature.

- The information must be provided in a format requested by the data subject. One copy should be issued to the data subject, or their legal representative and one copy should be retained by Stripes.
- Agree how the information is to be provided to the individual – this will be dependent on the volume of the information. Consider data security before issuing the information and seek advice if necessary.

Data Breach

A data breach is any security breach leading to accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data.

- We investigate breaches to identify necessary actions, which could include procedural changes or disciplinary actions in cases of negligence.
- We notify the ICO within 72 hours if a breach risks individuals' rights and freedoms. Significant effects may include discrimination, reputational damage, financial loss, or loss of confidentiality.

Data Retention

We keep data only as long as needed for business or compliance purposes. Generally, records are kept for 6 years after the accounting year they relate to, but some records may need longer retention due to legal requirements, storage costs, historical value, industry standards, or archival needs.