Data Protection Policy and Guidelines (GDPR)

This document sets out Escape Youth Services (EYS) policy on the protection of information relating to staff members, workers and volunteers. Protecting the confidentiality and integrity of personal data is a critical responsibility that EYS takes seriously at all times. EYS will ensure that data is always processed in accordance with the provisions of relevant data protection legislation, including the General Data Protection Regulation (GDPR).

KEY DEFINITIONS

Data processing

Data processing is any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Personal data

Personal data is any information identifying a data subject (a living person to whom the data relates). It includes information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers EYS possesses or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Sensitive personal data

Sensitive personal data is a special category of information which relates to a data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. It also includes personal data relating to criminal offences and convictions.

PRIVACY NOTICES

EYS will provide staff members and adults in care of service users with privacy notices setting out the information EYS holds about staff and members, the purpose for which this data is held and the lawful basis on which it is held. EYS may process personal information without staff/members' knowledge or consent, in compliance with this policy, where this is required or permitted by law.

If the purpose for processing any piece of data about staff/members should change, EYS will update privacy notices with the new purpose and the lawful basis for processing the data and will notify staff members of changes.

FAIR PROCESSING OF DATA

Fair processing principles

In processing staff/members' data the following principles will be adhered to. Personal data will be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that are clearly explained and not used in any way that is incompatible with those purposes;
- Relevant to specific purposes and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the specified purposes; and
- Kept securely.

Lawful processing of personal data

Personal information will only be processed when there is a lawful basis for doing so. Most commonly, EYS will use personal information in the following circumstances:

- when it is needed to perform staff members' contracts of employment;
- when it is needed to comply with a legal obligation; or
- when it is necessary for the EYS legitimate interests (or those of a third party) and staff members' interests and fundamental rights do not override those interests.

EYS may also use personal information in the following situations, which are likely to be rare:

- when it is necessary to protect staff members' interests (or someone else's interests); or
- when it is necessary in the public interest [or for official purposes].

Lawful processing of sensitive personal data

EYS may process special categories of personal information in the following circumstances:

- In limited circumstances, with explicit written consent;
- in order to meet legal obligations;
- when it is needed in the public interest, such as for equal opportunities monitoring [or in relation to the EYS occupational pension scheme]; or
- when it is needed to assess working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, EYS may process this type of information where it is needed in relation to legal claims or where it is needed to protect a staff member's interests (or someone else's interests) and the staff member is not capable of giving consent, or where a staff member has already made the information public. EYS may use particularly sensitive personal information in the following ways:

- information relating to leaves of absence, which may include sickness absence or family related leaves, may be used to comply with employment and other laws;
- information about staff members' physical or mental health, or disability status, may be used to ensure health and safety in the workplace and to assess fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits;
- information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, may be used to ensure meaningful equal opportunity monitoring and reporting; and
- information about trade union membership may be used to pay trade union premiums, register the status of a protected staff member and to comply with employment law **obligations.**

Lawful processing of information about criminal convictions

EYS does not envisage that it will hold information about criminal convictions. If it becomes necessary to do so, YouthBorders will only use this information where it has a legal basis for processing the information. This will usually be where such processing is necessary to carry out the EYS obligations. Less commonly, EYS may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect a staff member's interests (or someone else's interests) and the staff member is not capable of giving consent, or where the staff member has already made the information public.

EYS will only collect information about criminal convictions if it is appropriate given the nature of the role and where it is legally able to do so. Where appropriate, EYS will collect information about

criminal convictions as part of the recruitment process or may require staff members to disclose information about criminal convictions during the course of employment.

Consent to data processing

EYS does not require consent from staff members to process most types of staff member data. In addition, EYS will not usually need consent to use special categories of personal information in order to carry out legal obligations or exercise specific rights in the field of employment law. If a staff member fails to provide certain information when requested, EYS may not be able to perform the contract entered into with the staff member (such as paying the staff member or providing a benefit). EYS may also be prevented from complying with legal obligations (such as to ensure the health and safety of staff members).

In limited circumstances, for example, if a medical report is sought for the purposes of managing sickness absence, staff members may be asked for written consent to process sensitive data. In those circumstances, staff members will be provided with full details of the information that sought and the reason it is needed, so that staff members can carefully consider whether to consent. It is not a condition of staff members' contracts that staff members agree to any request for consent.

Where staff members have provided consent to the collection, processing and transfer of personal information for a specific purpose, they have the right to withdraw consent for that specific processing at any time. Once EYS has received notification of withdrawal of consent it will no longer process information for the purpose or purposes originally agreed to, unless it has another legitimate basis for doing so in law.

Automated decision making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

EYS may use automated decision-making in the following circumstances:

Where staff members have been notified and given 21 days to request a reconsideration.

Where it is necessary to perform a contract and appropriate measures are in place to safeguard staff members' rights.

In limited circumstances, with staff members' explicit written consent and where appropriate measures are in place to safeguard staff member rights.

If EYS makes an automated decision on the basis of any particularly sensitive personal information, staff members will be asked for explicit written consent unless processing is justified in the public interest. EYS will put in place appropriate measures to safeguard staff member rights. Staff members will not be subject to decisions that will have a significant impact based solely on automated decision-making, unless EYS has a lawful basis for doing so and has given staff members prior notification.

COLLECTION AND RETENTION OF DATA

Collection of data

EYS will collect personal information about staff members through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. EYS may sometimes collect additional information from third parties including former employers.

From time to time, EYS may collect additional personal information in the course of job-related activities throughout the period of employment. If EYS requires to obtain additional personal information, staff members will receive a fresh or updated privacy notice setting out the purpose and lawful basis for processing the data.

Retention of data

EYS will only retain staff members' personal information for as long as necessary to fulfil the purposes it was collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements (see guidelines set out below).

When determining the appropriate retention period for personal data, EYS will consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which the personal data is processed, whether EYS can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances EYS may anonymise personal information so that it can no longer be associated with individual staff members, in which case EYS may use such information without further notice to staff members. After the data retention period has expired, EYS will securely destroy staff members' personal information.

Data retention guidelines:

- General personnel records – duration of service + 5 years
- Disciplinary proceedings – duration of warning
- Notes of disciplinary proceedings – 3 years unless otherwise agreed
- Notes of disciplinary appeal – conclusion of appeal
- Annual and special leave record - 3 years
- Travel and other expenses – 5 years
- Sickness records - 3 years
- Termination of employment – 6 years
- References – 5 years
- Information on clients/individuals with whom the organisation has dealings with – 3 years from last contact

DATA SECURITY AND SHARING

Data security

EYS has put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed (see compliance section below).

Access to personal information is limited to those staff members, agents, contractors and other third parties who have a business need to know. They will only process personal information on EYS instructions and are subject to a duty of confidentiality. EYS expects staff members handling personal data to take steps to safeguard personal data of staff members (or any other individual) in line with this policy.

Data sharing

EYS requires third parties to respect the security of staff member data and to treat it in accordance with the law. EYS may share personal information with third parties, for example in the context of the possible sale or restructuring of the business. EYS may also need to share personal information with a regulator or to otherwise comply with the law.

EYS may also share staff member data with third-party service providers where it is necessary to administer the working relationship with staff members or where EYS has a legitimate interest in doing so. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services.