HACRO
The Hertfordshire Association for the Care and Rehabilitation of Offenders

HACRO
62-72 Victoria Street
St Albans
Herts, AL1 3XH

Tel. 01727 854727
E-mail: office@hacro.org.uk

HACRO Data Protection and Information Security Policy

This policy refers to the Data Protection Act 2018
Date 23.5.18
Number 4-3 rev 3

1. Introduction

HACRO is a registered charity dedicated to assisting offenders and their families. HACRO aims to ensure that its handling of information complies with best practice, with the Data Protection Act 1998, with the privacy principle in the Human Rights Act 1998 and with the requirements of the General Data protection Regulations which come into effect on 25th May 2018.

While this document aims to ensure that appropriate levels of confidentiality are applied to all information, in particular about individuals, at the same time HACRO aims to operate in an open way in matters of public accountability.

Principles underlying this document are:

- We aim to comply with all relevant legislation (e.g. Data Protection Act, Human Rights Act, Freedom of Information Act)
- We aim to apply a high level of security to data about clients and other individuals.
- Everyone within HACRO has a responsibility to ensure that data is held securely

*This document applies to all data held and processed within HACRO and should **not** be regarded as solely concerning data held or processed electronically.*

2. The Data Protection Act

The Data Protection Act requires that personal data shall be: adequate, relevant and not excessive for the purpose(s) for which they are held (the third principle); accurate and where necessary kept up to date (sixth principle); and not kept for longer than is necessary for its purpose(s) (fifth principle) and that, appropriate technical and organisational measures shall be taken against unauthorised or unlawful

processing of personal data and against accidental loss or destruction of, or damage to, personal data (seventh principle).

The General Data Protection Regulations require that the legal grounds for processing electronically held data are documented, and where Consent is a ground, that method of consent and its duration are recorded. Data subjects must also be informed about the use and transfer of their data and given an opportunity to withdraw consent.

There is a general requirement to hold personal data secure from unauthorised access or loss, and to make sure it is up to date. More stringent requirements apply to sensitive personal data.

3. In order to satisfy the requirements of Data Protection:

a. Where personal data is processed electronically, we must be able to show the reason why we are entitled to process that data.
b. Where the reason is by virtue of data subject consent, we must record the date and way that consent was obtained and make clear how it may be withdrawn.
c. We must ensure that personal; information cannot be accessed by unauthorised persons
d. We must ensure that the information is secured against accidental loss or deletion.

4. **General Office Security**

General access to HACRO office space is controlled as it is integrated into the National Probation Service offices in St Albans so that only authorised visitors may enter.

5. Security of data on paper

All sensitive paper records (grant applications, client, employee or volunteer personal details etc) are secured at the end of each working day within lockable storage cabinets.

6. Transfer of information outside the workplace

a. We will not sell or give address lists to third parties unless required to do so by law, or in order to facilitate legitimate mail distribution by mail providers.
b. Paper-based information about confidential matters or about individuals which is sent by post is enclosed in a sealed envelope and marked for the personal attention of the recipient.
c. Any confidential information about clients or volunteers sent by email is formulated in such a way that the identity of the individual concerned is not revealed.
d. **Specific considerations to handling information**:
    i. All Trustees, employees and volunteers must consider that certain information passed to HACRO and held by HACRO is likely to be highly confidential or sensitive. This information may not always be marked “confidential”, although thought should be seriously given to do so when appropriate. However, sensible individual judgement should be applied, and if in doubt, advice sought as to the nature of said information, and such information should not be shared with other individuals, agencies or authorities unless appropriate permissions or authorisations are obtained. This process cannot be prescriptive as each situation will be different and so the need to share the information and the impact on other parties must be

carefully considered. Historically trustworthy bodies who need the information to allow our activities to continue would normally be considered approved.

ii. Before agreeing to any market or publicity referring to HACRO, the person involved must seek agreement from the Chair of HACRO and if not available one of the senior trustees. Normally such a decision would wait until the Chair was available.

7. Data Backup

The official storage location for most of HACRO's data is on the OneDrive which, being cloud-based, is backed-up automatically. Any further data relating to individuals kept on any HACRO pc or lap-top has to be backed-up to a password protected backup disc or encrypted memory stick every day.

8. Passwords

a. Every computer user is to have an individual System Log On password
b. Passwords are to be minimum of 6 (six) characters using a combination of letters, numbers, lower and uppercase
c. Users are to Log Off whenever they leave their PCs unattended.
d. Password protection to be enabled on all PCs after 20 minutes of inactivity
e. Users are not to divulge or share their password with other users
f. Laptops should have a separate hard disk password.

9. Software/ Copyright

All members of HACRO have to abide by the legal restrictions on the use of copyright material, particularly proprietary software.

No new software is to be introduced into a HACRO PC and/or Network without prior authorisation from the Trustee responsible for IT, or, if unavailable, the Chair of the HACRO Committee.

10. Third party access

All members of HACRO shall ensure that breaches of data security are prevented by ensuring third parties (Cleaners/contractors/ temporary staff/ IT repair contractors/family members of volunteers) do not have unauthorised access to sensitive information.

a. Where a computer is shared with others (e.g. family members) HACRO work shall be done under a user name not accessible to other people, and HACRO data in folders should be encrypted.
b. Data is to be kept secured at all times. Extra consideration is to be given to assets / media taken off- site (Laptops / Backup disks / Paper Files etc.)
c. On-site contractors should not be left unsupervised.
d. PCs are to be erased of all data if they are required to go off-site for maintenance or repair.

11. Anti-virus / Firewall

a. All PCs are to have the appropriate Anti – virus software installed.

b. Internet accessible PCs are to have their Anti-Virus protection update automatically when online.
c. Only PCs protected by 'Firewall' software, or by a hardware Firewall are authorised to access the Internet.
d. It is the responsibility of all pc users to ensure the anti-virus software is up to date.

12. . Incident reporting.

All breaches of information security shall be reported to the Chief Executive Officer (CEO) of HACRO or Trustee responsible for IT as soon as possible. In some instances, immediate action may be necessary in relation to an incident, but initial reporting must take place no later than the end of the working day on which the incident is discovered. Potential breaches (i.e. vulnerabilities) including concerns about software should be reported in the same manner.

The object of this process is to minimise harm from any incident and to minimise the risk of such an incident recurring by giving consideration to changes of procedures.

13. Disciplinary Process

Contravention of these practices and procedures may be viewed as an offence under staff disciplinary procedures.