DATA PROTECTION AND SECURITY POLICY

1. Data protection principles

Healthwatch Birmingham (HWB) is committed to processing data in accordance with its responsibilities under the General Data Protection Regulation (GDPR).

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General provisions

a. This policy applies to all personal data processed by HWB.
b. Chipiliro Kalebe-Nyamongo is the Data Protection Officer who is responsible for HWB's ongoing compliance with this policy.
c. This policy shall be reviewed at least every three years.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, HWB shall maintain a Register of Personal Data (the Register).
b. The Register shall be reviewed at least every three years.

c. Individuals have the right to access their personal data and any such requests made to HWB shall be dealt with in accordance with the legislation. Subject Access Requests will be responded to within 30 days.
d. HWB will inform data subjects when it shares data with other organisations, unless data sharing without consent is allowed by the law, and it will require these organisations to provide appropriate security to protect the data shared.

4. Lawful purposes

a. All data processed by HWB must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. HWB shall note the appropriate lawful basis in the Register.
c. Special data is data about an individual's:
    i. Racial or ethnic origin
    ii. Political opinions
    iii. Religious or similar beliefs
    iv. Trade union membership
    v. Physical or mental health
    vi. Sexual life
d. All special data processed by HWB must be done on one of the following ten lawful bases for processing special data, including:
    i. consent
    ii. employment, social security or social protection law obligations or a collective agreement
    iii. protection of vital interests if the individual cannot give consent
    iv. processing by not-for-profit body with political, philosophical, religious or trade union aim where processing relates to members or former members
    v. data made public by the data subject
    vi. necessary for legal claims or where courts are acting in their judicial capacity
    vii. necessary in public interest if proportionate to aim pursued and where appropriate safeguards
    viii. necessary for preventative or occupational medicine, to assess working capacity of employee, medial diagnosis, provision of health or social care or treatment or management of health or social care systems and services
    ix. necessary for the public interest in public health, eg to protect serious cross border health threats or to ensure high standards of healthcare and medicinal products and devices
    x. necessary for archiving in the public interest or for scientific and historical research or statistical purposes (see ICO guidance for more information)
e. Where consent is relied upon as a lawful basis for processing data or special data, evidence of opt-in consent shall be kept.
f. Where communications are sent to individuals based on their consent, the

option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in HWB's systems.

5. Data minimisation

a. HWB shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. HWB shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, HWB shall put in place a Retention Policy for each area in which personal data is processed.
b. This will be reviewed at least every 3 years.

8. Security

a. HWB shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security is in place to avoid unauthorised sharing of information.
c. When personal data is deleted this will be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.
e. Annex A to this policy sets out HWB's specific data security rules to protect personal data.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, HWB shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

ANNEX A – DATA SECURITY

Adequate data security is essential to meet the principles of the General Data Protection Regulation and the following safeguards are in place at HWB:

1. Each of the electronic databases has built-in IT security, backed up by copying to secure storage each night.
2. External access to the databases is limited by [security firewalls and individual passwords]
3. Passwords expire after [90 days] and have to be [complex to be accepted on the network].
4. Only staff who have to have access to databases for their work have the required logins and passwords to access such databases.
5. Although workstations automatically lock if left inactive for a specific period, users are advised to always lock their workstations when moving away from their desk (windows key and L on a PC).
   Data stored on a network drive is backed up each night.
6. If logins and passwords are compromised then these are changed as soon as possible.
7. A range of specialist databases exist which contain varying levels of personal and special information. [Special rules exist for databases containing special information]
8. All other personal or sensitive data that may be held in local, small-scale documents, for example spreadsheets and word documents, must be password protected and restricted to essential users.
9. Personal or sensitive data should not be copied or downloaded to a lap-top computer for local processing without the agreement of the Data Protection Officer and where IT Support Services have agreed that the data will be sufficiently protected and where this is necessary.
10. Personal or sensitive data should not be stored on flash-drives, CD-ROM or other external devices.
11. Data taken out of the office, for example for home working or for meeting, must be [signed out] and must always be done only with the prior agreement of the Data Protection Officer. If you have any concerns about data security of personal data taken offsite, please raise these with the Data Protection Officer.
12. Hard copy data will be protected in locked filing cabinets. Only those who need to have access to the data will be given access to the key.
13. Data are retained and disposed of according to need and to agree retention periods set out in the Retention Periods Statement. The overarching principle is that data should only be retained and stored for as long as such data have a legitimate purpose, and as specified in the Retention Periods Statement and the Privacy Statements and thereafter they should be disposed of securely.
14. At the end of the retention period, data should be disposed of and/or destroyed. Manual files should be shredded and disposed of in designated confidential waste sacks if appropriate. Electronic data should be deleted from

central systems by the individual responsible for the data after liaising with the [IT Services team].