# Data protection and cyber security

1. Introduction

(HTA/HTAF) take the protection of individuals data seriously and recognise the challenging environment.

2. Associated policies are:

    a. Social media policy;
    b. Cyberbullying policy;
    c. Privacy statement;
    d. POPIA Compliance Policy;
    e. PAIA Compliance Policy.

3. Background

    This policy responds to three imperatives

    a. The need for a data protection policy to comply with the UK Data Protection Act (1998) and in South Africa, the Promotion of Access to Information Act No. 2 Of 2000 (PAIA) and Protection of Personal Information Act No. 4 of 2013 (POPIA). These obligations of require specific actions and procedures to be in place.
    b. The need to respect the privacy of those who entrust us with their personal information.
    c. The growing risk from the use of mobile computing and increasing threat of cyber-attack. Risks from mobile computing result from:

        i. Data theft;
        ii. Device theft;
        iii. Malware, spyware and viruses;
        iv. Mixing data protected under The Act with an individual's own data;
        v. Device loss;
        vi. Change of device.

4. General Policy statement
    a. (HTA/HTAF) are, at times, required to collect, process and maintain certain personal and sensitive data about living individuals for the purpose of furthering their work.
    b. (HTA/HTAF) are committed to protecting the rights and privacy of individuals (including staff, members, adherents, supporters and those using our premises).
    c. The data policy is determined by the UK Data Protection Act 1998 and PAIA and POPIA.
    d. Personal and sensitive personal data shall be processed fairly and lawfully and that the data subject has given their consent to the processing.
    e. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

f. There should be “no surprises” as to how data is being used, i.e. people must be able to know how their data will be used.
g. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
h. Personal data shall be accurate and, where necessary, kept up to date.
i. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
j. Personal data shall be processed in accordance with the rights of data subjects under relevant legislation.
k. 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.
l. All computers and devices will have industry standard virus scanners and malware protection.
m. It is the responsibility of everyone working with, and on behalf of, (HTA/HTAF), and all those holding any office or having access to personal information, to ensure that data security is not compromised and that any personal data they hold in their area of responsibility is secure at all times.
n. Personal data is not disclosed either orally or in writing without the specific consent of the data subject or their authorised nominee.
o. The consent of the data subject must be secured before collecting or processing personal data and the data subject must be informed of the purposes for which their personal information will be used, and they must be given the opportunity to opt-out. *N.B. The European Data Protection Directive defines consent as “…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”,* meaning the individual may signify agreement other than in writing. However, non-communication should not be interpreted as consent.
p. Wherever practically possible consent should be obtained by the completion of a data collection form. There are however, routes where consent is deemed to have been given. They are where information has been “freely and willingly” given, e.g. via sending an email, or where a “legitimate interest” has been recognised. Both these routes should be regarded as exceptions.
q. Someone freely and willingly sending an email, text or phoning (HTA/HTAF) is deemed to have given their consent to that email address or phone number being held and used for purposes in accordance with the Privacy Statement.
r. Any data collection activity will specify the purposes for which the data is being collected.
s. Data will be held for the minimum time required and will be safely and securely destroyed after that date.
t. The minimum amount of data will be collected and processed.
u. Any computers or devices which have stored (HTA/HTAF) data will have the data on their storage devices securely destroyed prior to them being used by another party.
v. All individuals who are the subject of personal data held by (HTA/HTAF), either in paper based systems or electronically, are entitled to:

i. Ask what information is held about them and why;
ii. Ask how to gain access to it;
iii. Be informed about how they can keep it up to date;
iv. Be informed what (HTA/HTAF) is doing to comply with it obligations under The Act;
v. Require that data be deleted;
vi. Require that incorrect data be corrected;
w. The right to access is subject to certain exemptions set out in The Act. Any person wishing to exercise their right must make a request in writing to the Chair of (HTA/HTAF). The charge for such is determined periodically by appropriate Boards.
x. All requests for access will be executed in full within 40 days of receipt.