****

 **Mind in Haringey**

 **Information security policy**

**April 2023**

 **Mind in Haringey Information Security Policy**

1. **Scope of policy**

This policy applies to;

 All staff employed by Mind in Haringey consultants, agency workers, contractors,

students, trainees, temporary placements who have access to

information systems or assets belonging to the organisation.

 Other individuals and agencies who may gain access to data, such as

non-executive directors, volunteers, visiting professionals or

researchers, and companies providing information services to Mind in Haringey .

This policy will be supported by system-specific security policies, technical

standards and operational procedures, which will ensure that its

requirements are understood and met by all affected parties.

**2.Information Security Principles**

The core information security principles are to protect the following information/data

asset properties:

 Confidentiality (C) – protect information/data from breaches, unauthorised

disclosures, loss of or unauthorised viewing.

 Integrity (I) – retain the integrity of the information/data by not allowing it to

be modified.

 Availability (A) – maintain the availability of the information/data by protecting

it from disruption and denial of service attacks.

In addition to the core principles of C, I and A, information security also relates to the protection of reputation; reputational loss can occur when any of the C, I or A

properties are breached. The aggregation effect, by association or volume of data,

can also impact upon the Confidentiality property.

**3.Information Assets**

Mind in Haringey will ensure that:

 all information assets under its control are identified and documented in

an asset register;

 all information assets for which they are responsible are reviewed to

identify potential threats to the system, and the likelihood of those

threats occurring;

 the cost of countermeasures against perceived threats is commensurate

with threats to security, the value of the assets being protected and the

impact of security failure;

 all staff are fully trained in the use of the systems that they are required

to operate;

 Mind in Haringey’s electronic information assets are protected from the

threat of viruses and other malicious software;

 business continuity plans are in place to protect critical business

processes from the effects of major failures of IT systems or other

disasters.

**4. Computer Hardware & Software**

Authorised hardware and software , Only hardware approved by Mind in Haringey may be used or connected to its network. Any unauthorised hardware found will be removed.

Unauthorised software must not be used on Mind in Haringey’s equipment or on its network. Any unauthorised software found will be removed and may result in

disciplinary action.

Only authorised staff may install, modify or upgrade hardware or software

belonging to, or provided by the organisation.

All software licenses must be held by the IT department as this is required for

the asset register and also should any reinstall be necessary.

**5.Use of personal equipment**

Personal equipment must not be used on Mind in Haringey’s network for the

purpose of carrying out organisational business. Encryption controls may

impact on the running of personal equipment which in turn may result in

permanent damage to the device. Such personal equipment may include (but

is not exhaustive) PDAs, smart phones, laptops, tablets and external hard

drives.

 **6.Information storage and backup**

Staff are responsible for ensuring that information they process is saved

appropriately. Where a staff member has network access, all information must

be saved to their network drive which is automatically backed up.

Staff are advised that the authorised encrypted memory stick is only for the

transfer of information and the original content must be saved to the network.

**7.Access Controls**

All staff wishing to access Mind in Haringey’s network must firstly accept the

user agreement. In doing so, the user agrees to abide by the terms and

conditions stated as well as the policies of the organisation.

No one shall be granted access to an information system that does not

require that access as part of their work for the organisation.

Any access granted must be approved by the relevant IAO to ensure that access is

limited only to what is required.

**8.Passwords**

The primary form of access control for computer systems is via password.

Each member of staff using a computer system will have an individual

password. Sharing of passwords by both the person who shared the password and the person who received it is an offence under the Computer Misuse Act 1990.

All staff must follow robust security practices in the selection and use of passwords.

These will include;

 Logon details are not to be shared or used under supervision even in

training situations

 ensuring strong passwords are used i.e. using a minimum 8 digit

combination of letters, numbers and special characters (!?£&%$ etc) and

to ensure that consecutive passwords are not used e.g. mypassword1,

mypassword2, mypassword3 etc.

 not writing down passwords where they can be easily found, i.e. on

sticky notes next to their workstation

 ensuring passwords are changed when prompted

 changing their password immediately if they suspect it has been

compromised and reporting the incident using the organisation incident

reporting system

 using the Microsoft two way authentication app for Microsoft package and VIEWS CRM system and not basing their password on anything that could be easily guessed by another, such as their own name, make of car, car registration, name of pets etc.

**10.Access to other staff members’ data**

**Email**

In cases where access to other staff members’ login details is necessary eg

due to illness absence, permission can only be given to the Line Manager to

access the account through contact with the IT Services. Staff must ensure that they provide access to their Line Manager or other appropriate person in cases of planned absences.

**Personal Folders**

In cases where there is a requirement for access to data e.g. due to illness,

then permission must be sought from the folder owner before access can be

granted by the IT Services.

**Remote Access and Mobile Working**

Staff must not attempt to connect to the network remotely without permission

to do so. Staff wishing to gain remote access to the network must do so in accordance with the remote access requirements.

**11.Information Incidents**

All incidents relating to information security must be reported using the

standard procedures for incident reporting.

The reporting of incidents is important to ensure that appropriate actions are

taken to minimise impact, avoid reoccurrence and to share any lessons

learned. In the case of serious incidents that Mind in Haringey may have to secure

digital forensic evidence, for example, on a hard drive to prevent this from

being tampered with during formal disputes or legal proceedings.

**12.Internet and Email Security**

When accessing the Internet or email the following must be adhered to;

 Before using the Internet, Intranet or email for the first time all staff must

accept the terms and conditions of the use;

 No illicit or illegal material may be viewed/downloaded or obtained via

the Internet or email;

 Any material downloaded must be virus checked automatically by the

system’s anti-virus system.

 The user will make their system available at any time for audit either by

the IT department or internal and external audit.

**13.Transferring information and equipment**

It is important that the utmost care is exercised when transferring

information, especially information of a confidential nature e.g. staff, patient

or service user information. This includes transferring information by

telephone (voice and text), email, courier and post.

Regular exchanges of personal information must be governed by information

sharing protocols or data processing agreements within contracts.

Staff must not leave any property belonging to the organisation, including

laptops, portable devices, mobile telephones, records or files in unattended

cars or in easily accessible areas for extended periods.

These must either be secured within premises under the organisation’s control, or where this is not practicable secured within the employee’s home. Where an overnight stay for work purposes is required the same principles apply.

In instances where equipment or records are unavoidably left unattended for

short periods e.g. calling at another base, making an unscheduled stop, the

staff member must assess the potential risk to the equipment whilst it is

unattended.

**12.Systems Development, Maintenance & Security**

The organisation must ensure that security requirements are built into

systems from the outset. Suitable controls must be in place to manage the

purchase or development of new systems and the enhancement of existing

systems, to ensure that information security is not compromised.

IAO implementing or modifying systems are responsible, in collaboration

with IT contractor to ensure that:

 that all modifications to systems are logged and up to date

documentation exists for their systems and follow change control

procedures

 contracts with suppliers include appropriate confidentiality clauses

 they complete a risk assessment with the support of the Information

Governance Lead

 that vendor supplied software used in systems, is maintained at a level

recommended by the supplier.

 that physical or logical access is only provided to suppliers for support

purposes when necessary, and must be with IAO and IT approval

 that all supplier activity on the system is monitored.

 that copies of data must retain the same levels of security and access

controls as the original data.

**13.Business Continuity Plans**

Business continuity plans must exist for each service that allow critical

systems to be maintained and to restore critical systems in the event of a

major disruption e.g. through a disaster or security failure.

It is the responsibility of the IAOs to ensure that their individual business

continuity plans are regularly updated to reflect changes in service delivery.

Business continuity plans should be tested annually.

**14.Implementation**

All managers are responsible for ensuring that relevant staff within Mind in Haringey have read and understood this document and are competent to carry out their duties in accordance with the requirements described.

 **15.Policy Review**

The Data Protection Officer is the owner of this document and is responsible for

ensuring that this policy is reviewed annually. This policy was approved by CEO and a Senior Manager.

This policy was ratified by Trustees on April 2023