Information Security Policy

Name	Reason for change	Date
Nazmul Ahmed	**Original author**	June 2019

Approval process for current version

Presented to	Date	Outcome

Contents

1. Introduction

This policy forms part of our approach to effective business management, personnel management, and data protection. It describes some of the specific measures we have in place to ensure that we keep information and IT resources secure and to ensure they are used appropriately. Additional arrangements may be set out in other policies, be built into the way we do business, or notified to staff from time to time.

Poplar HARCA provides ICT resources to enable and support individuals to progress and do their jobs. ICT resources include, but are not limited to, applications, social media, internet, software, hardware, phones, computers and tablets.

Poplar HARCA also allows access to its ICT resources by personal devices being used for work purposes.

Technology and the law change frequently and every effort will be made to update this policy as necessary; and to alert individuals to the updated version.

Individuals who use or access Poplar HARCA's ICT resources are responsible for ensuring they comply with this policy and the relevant law when they do so.

Individuals who use social media in a personal capacity must comply with the social media section of this policy even when they are accessing social media through applications or hardware devices, including desktops, laptops, tablets and mobile phones, which have not been issued by Poplar HARCA.

Line managers must ensure contractors, consultants, agency workers, volunteers, residents and anyone else they are responsible for who uses or accesses Poplar HARCA's ICT resources, and/or social media, are aware of this policy.

If anything in this policy is unworkable; or if any aspect of it is not understood; the individual must notify their manager or a member of the People & Development (PaD) Team as soon as possible.

Failure to comply with any aspect of this policy may be investigated under Poplar HARCA's disciplinary policy as gross misconduct and could lead to dismissal.

2. Information Security

Information (including personal data) about our staff, tenants, and business is an asset of Poplar HARCA's. We therefore take a risk based approach and put in place measures that

keep that information safe and secure in use, and protect it from unauthorised access or loss or damage.

3. Information Security – Incident Management

We have a process for reporting, logging, managing, and learning from information security incidents (including potential 'Personal Data Breaches' for the purposes of data protection law). If a member of staff is involved in, or becomes aware of, a suspected incident involving data loss or unauthorised access, or a complaint is made about our information security practices, Business Support must be contacted immediately via **BusinessSupportTeam@poplarharca.co.uk**

4. Information Security – Information Technology

Poplar HARCA maintains a variety of measures to ensure that its IT systems and data held electronically is kept secure. This includes:

1) Encryption of all mobile devices (including tablets, laptops and work phones) and the facility to wipe such devices remotely.

2) Antivirus and firewall protection and other network security measures.

3) Restrictions on websites that may be visited on Poplar HARCA systems and downloads that may be made.

4) Secure remote log-in arrangements.

5) Role-based access and restrictions on systems and storage.

6) Monitoring usage of user accounts.

7) Secure printing.

Other parts of this policy describe measures applicable to staff using our IT systems.

5. Information Security

The nature of our business means that we receive visitors and certain parts of our facilities need to be open to members of the public during our opening hours.
Security perimeters (barriers such as walls, card controlled entry gates/doors and manned reception desks) are used to protect areas that contain sensitive information and information processing facilities.

Physical security for offices, rooms, and facilities is applied. Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access. Access points such as front-of-house, delivery and loading areas and other points where unauthorised persons may enter the premises are controlled and, as far as possible, isolated from information processing facilities to avoid unauthorised access.

The date and time of entry and departure of visitors from our secure area is recorded in a log book, and all visitors are supervised in secure areas unless their access has been previously approved and they are given a daily swipe card which is returned the same day; they are only granted access for a specific, authorised purpose, and/or accompanied by an appropriate member of Poplar HARCA staff.
Access to areas where sensitive information is processed or stored is controlled and restricted to authorised persons only; swipe cards and digital pin codes are used to authorise and validate all access. Staff work in teams, and some teams may be located in separate parts of our buildings to increase security arrangements.

All employees, contractors and third party users are required to display passes on entry to the building. All staff must immediately notify security personnel if they encounter unescorted visitors within the secure area.

6. Information Security – Clear Desk

Even though most staff work in a secure environment (i.e. to which the public do not have access), we will take steps to minimise the risk that papers and devices are lost, stolen or inadvertently picked up. We operate a 'paper-light' office and information which is no longer needed should be stored securely or put in a confidential waste bin. Desks should be clear at the end of the day/when a staff member leaves, and uncollected printing shredded. Meeting rooms should be reset for the next users at the end of each meeting, with no confidential information (e.g. on flip-charts or video screens) on display.

7. Information Security – Out of office

The very nature of our work means that our staff will need to go out to visit residents and partner organisations, and may take information with them or receive information whilst out and about. We also may allow staff to work remotely/in an 'agile' way.

We have invested heavily in encrypted IT systems that can be used remotely, and wherever possible this equipment should be used in preference to taking hard-copy files or paperwork out of the office. Privacy screens are available for electronic devices.

All staff are responsible for ensuring that information in their possession and devices assigned to them, are secure when out of the office. Items (whether hard-copy or

electronic devices) should never be left unattended, and particular care should be taken on public transport and in other busy environments.

Where particularly sensitive information is being handled, staff should consider how they can minimise the amount of time that the information in question is held out of the office. That may mean, for instance, making a specific visit to a property and then returning to the office straight away, rather than visiting multiple properties (and having hard-copy information for all visits in possession at the same time).

Staff should return paperwork to the office no later than the end of each day (rather than take papers home with them).
No papers should be disposed of in bins or recycling away from the office.

We operate a 'clean dashboard' policy and no items should be left in vehicles overnight.

8. Information Security – hard-copy correspondence

We will take a risk-based approach to sending out hard-copy correspondence, and in particular we will use more secure means of postage/delivery (such as special delivery, courier or hand delivery; double-bagging envelopes, etc.), where appropriate, to ensure that information is not exposed to risk once it has left our office. Where staff are responsible for sending correspondence out, it is vital that the information, and any enclosures, are checked for accuracy prior to being sent out. In particular, this includes drawing down and checking addresses from Streetwise and our databases rather than copy-typing addresses, and checking that the right papers are included in the envelope. Personal and private and confidential correspondence should be marked as such.

Where sharing large amounts of (sensitive) information with other organisations, consideration should be given to sending this in an encrypted electronic format, rather than hard-copy.

9. Information Security – Out of the Office

The very nature of our work means that our staff will need to go out to visit residents and partner organisations, and may take information with them or receive information whilst out and about. We also may allow staff to work remotely/in an 'agile' way.

We have invested heavily in encrypted IT systems that can be used remotely, and wherever possible this equipment should be used in preference to taking hard-copy files or paperwork out of the office. Privacy screens are available for electronic devices.

All staff are responsible for ensuring that information in their possession and devices assigned to them, are secure when out of the office.

Items (whether hard-copy or electronic devices) should never be left unattended, and particular care should be taken on public transport and in other busy environments.

10. Information Security – On the Phone

Staff should be mindful of:

1) Being overheard on the phone by third parties; and
2) Identity fraud/misrepresentation by phone leading to information being disclosed.

We may ask security questions to verify the identity of the caller. If in doubt, staff should consider terminating the call, sending information to a pre-assigned address or email account, or calling back on our pre-saved number for the person calling us.

11. Information Security – Email

We recognise that email is often the most effective and economical way of communicating in writing with partner organisations, colleagues and residents. However, the instantaneous nature of emails and the facility to attach information to them, presents a particular risk.

We may implement various solutions to:

1) Limit 'autocomplete' functions on emails being sent
2) Have options available for secure email (to include encrypted emails and password restrictions for attachments).

It remains the responsibility of staff to check that the email is going to be sent to the intended recipient and that any attachment is appropriate.

Bulk-emailing, and the use of 'BCC' functions is discouraged. Talk to IT if you need help sending the same information to a large number of recipients.

It is against Poplar HARCA's policy to send material to an external email address or personal device for the purpose of working outside of Poplar HARCA's provided systems. If a member of staff needs additional technology to do their job, this should be discussed with IT. We may use tools to monitor and record all email traffic using our email servers. Please note, ALL emails and network storage areas are able to be viewed by selected members of the IT team for the purposes of maintaining information security or carrying out investigations as required. For the avoidance of doubt, this includes emails that are non-work related and of a personal nature sent to or from a Poplar HARCA email address, instant messenger communications and text messages, etc. We may use software tools to automatically alert us to potential breaches of firm policy, these tools are specifically designed to identify breaches using rules based analysis, algorithms and machine.