# Information Security
# Policy and Procedure

**Valid From:** January 2014
**Review Due:** January 2019

King's Building
16 Smith Square
London SW1P 3HQ

T: 020 7937 1166
E: policyresponse@lookahead.org.uk

Look Ahead
CARE, SUPPORT AND HOUSING

# Our mission

**Working with people to make choices, achieve goals and take control of their lives through high quality care, support and housing.**

# Our values

**Excellence**

**Aspiration**

**Partnership**

**Trust**

**lookahead.org.uk**

**Services we would be proud for our loved ones to receive**

# Contents

# Policy

## 1 Scope

1.1 This Policy shall apply to:

- All automated information systems under the direct control of Look Ahead.
- All employees and agents of Look Ahead
- All employees and agents of other organisations who directly or indirectly make use of or support the use of information systems under the direct control of Look Ahead.

1.2 As stated, this policy is aimed specifically at information systems but it should be read in conjunction with the other policies in force on confidentiality, physical security and quality as well as the more specific information system security policies which govern the use of particular systems.

## 2 Introduction

2.1 Look Ahead holds and manages a great deal of information, much of it personal and confidential, without which it could not function. The purpose of information security is to enable information to be shared between those who need to use it while protecting information from unauthorised access and loss.

2.2 In keeping with information governance guidelines, this policy promotes the sharing of information, whilst ensuring the proper protection of that information in accordance with the prevailing legislative requirements.

2.3 This policy and procedure provides a framework of controls to ensure a secure operating environment thereby reducing risk to the organisation, its staff, contractors and service users.

2.4 Disclosure or misuse of personal data will be treated as a serious offence, which may result in disciplinary action in accordance with Look Ahead's Disciplinary Procedures.

2.5 All staff members are bound by this policy, access to any Look Ahead IT or communication system or equipment is only under the condition of acceptance of these conditions. This policy is therefore **VERY IMPORTANT**. If you have any queries relating to it or your personal situation please contact the IT Helpdesk or the HR department.

## 3 Definitions

### Hardware

3.1 Any ICT equipment provided by Look Ahead (including PC's, laptop computers, mobile devices, phones). In all cases the term 'PC' can be applied to a terminal, remote access portal, mobile device or phone capable of access Look Ahead Systems

### Software

3.2 Any programme provided, licensed or purchased by Look Ahead Housing and Care

### Internet

3.3 Public unregulated information resource.

### E-mail

3.4 Electronic method of sending and receiving messages.

### Removable Devices

3.5 USB Keys, External Attached Devices, Media Card Readers.

### Remote Access

3.6 The capability to access Look Ahead data or systems from a non-Look Ahead location or site.

### Home Computer

3.7 Any computer that is not owned by Look Ahead but is used by a Look Ahead employee to access information remotely.

## 4 Policy Objectives

4.1 Key Issues addressed by the Information Security policy are:

### Confidentiality

4.2 Ensuring that information is accessible only to those authorised to have access

### Integrity

4.3 Safeguarding the accuracy and completeness of information and associated assets when required

### Availability

4.4 Ensuring that authorised users have access to information and associated assets when required

### Risk Assessment

4.5 Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence

### Risk Management

4.6 Process for identifying, controlling and minimising or eliminating security risks that may affect information systems, for an acceptable cost.

4.7 The Objective of this policy is to establish and maintain the security and confidentiality of Information Systems, applications and networks owned or held by Look Ahead by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other documents.
- Describing the principles of security and explaining how they shall be implemented within the Company.
- Introducing a consistent approach to security and ensuring that all members of staff understand their responsibilities.
- Creating and maintaining within the Company a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

# 5 Responsibility for Security

5.1 Each individual user of any part of the Look Ahead information system has responsibility to comply with the security requirements that may be in force. They shall generally strive to ensure that the confidentiality, integrity and availability of the Look Ahead information system(s) is preserved to the highest standard and ensuring that no breaches of IT security results from their actions.

5.2 This policy and procedure shall be maintained, reviewed and updated in accordance with the risk management strategy of Look Ahead Housing and Care.

## Management Responsibilities

5.3 It is the responsibility of managers to ensure the following with respect to their staff:

- All current and future staff should be instructed in their security responsibilities
- Staff using computer systems/media must be competent in their use
- Staff must not be able to gain unauthorised access to any IT systems, thus compromising data integrity.
- Managers should determine which individuals are to be given authority to access specific computer systems or data sources. The level of access to specific systems should be on a job function needs, independent of status.
- Managers should implement procedures to minimise the organisation's exposure to fraud, theft or disruption of its systems, such as segregation of duties, dual control or staff rotation in critical susceptible areas.
- Managers should ensure that the relevant system managers are advised immediately about staff changes affecting computer access (eg, job function changes, leaving department or organisation) so that systems access may be withdrawn or deleted.
- Managers must ensure that a up to date asset register is held locally for all staff assigned a mobile working kit (Netbooks, dongle & signature pad) , mobile phones and laptops.
- Managers must ensure that all contractors undertaking work for or on

behalf of Look Ahead have signed 3rd party access agreements.

## 6 Permitted Use of Look Ahead's Computer Network and Equipment

6.1 All specified staff, 'the users' (refer to user list maintained by IT) have access to any device from which Look Ahead data or systems may be accessed and/or Look Ahead's computer network. IT maintains the control list of all approved post holders and users.

6.2 The computer network and all equipment are the property of Look Ahead and are to be used in accordance with this policy. Users are provided access to computers and the network to assist them in the performance of their jobs.

6.3 All users have a responsibility to use Look Ahead's computer resources in a professional, lawful and ethical manner and in accordance with procedures and the Data Protection Act 1998. (**Appendix 7**).

6.4 All staff have access to appropriate training on the use of Look Ahead's computer system, to assist them to fully utilise IT in the fulfilment of their role. This is provided through Look Ahead's IT Training Courses, and other ad hoc training sessions.

6.5 Look Ahead is committed to use only authorised software.

6.6 All new software and hardware purchases are to be approved by the Head of IT or IT Manager with reference to the IT Strategy. Larger software applications need to be approved by SMT following a cost benefit analysis.

6.7 There are a small number of laptops available for short term loan to staff for business purposes which have to be signed for. This policy also applies to the use of the laptops.

6.8 Remote working from home – this policy also applies to staff remote working from home for business use.

## 7 Network Access Form

7.1 New users are required to sign the Network Access form (**Appendix 1**), which acts as an acknowledgement that this policy has been read and understood by the staff member. This policy is distributed to all new employees before starting at Look Ahead. **The Declaration in Appendix 1 should be signed and returned to HR on the first day of commencing work at Look Ahead.**

7.2 The original declaration should be placed on the user's personal file in HR and a copy given to the IT Team for audit records.

7.3 Users cannot be given access to any IT systems unless this form has been completed.

7.4 Short term temporary staff can be given access to the network with the authority of their line manager provided they have been made aware of the content of this policy.

7.5 Employees or agents should not attempt to access and Look Ahead IT resource without signing and returning the compliance forms.

# 8 Computer Network Use Limitations

## Prohibited activities

8.1 Look Ahead's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g. viruses, Trojan horse programmes, etc.) or any other prejudicial materials.

8.2 Look Ahead expressly bans the use of the computer network to send any defamatory, obscene or discriminatory material and/or any use of the e-mail system to harass members of staff in any way. All computer usage must comply with Look Ahead's Harassment and Bullying at work Policy and Procedure.

8.3 Essential personal use of Look Ahead's equipment is permitted in an emergency at any time, if such use does not a) interfere with the user's or any other employee's job performance; b) have an undue effect on Look Ahead's network's performance; c) or violate any other policies, provisions, guidelines or standards of this agreement or any other of Look Ahead's.

8.4 Personal devices such as PDA's, tablets or smartphones should not be connected to the network or any Look Ahead PC without the prior permission of the IT Team.

8.5 Employees shall not stop, uninstall or attempt to defeat any the security or monitoring measures put in place by the IT team including Virus checking, proxies, logs, etc.

8.6 All employees and visitors to the Company, including suppliers, contractors and consultants must not connect laptop computers or any other IT equipment to the Look Ahead network or IT Infrastructure. It is the responsibility of the Look Ahead employee who oversees the visitor to ensure that this does not occur.

8.7 Non-emergency private use should be minimal and in the employee's own time, unless unavoidable. Any use should comply with the spirit of this policy.

8.8 Employees own time is normally deemed to be their lunch break or outside working hours.

8.9 Further, at all times users are responsible for the professional, ethical and lawful use of the computer system. Personal use of the computer is a privilege that can be revoked at any time.

## Illegal copying

8.10 Users may not illegally copy material protected under copyright law or make that material available to others for copying.

8.11 Users are responsible for complying with copyright law and applicable licence agreements that may apply to software, files, graphics, documents, messages, and any other material to be downloaded or copied.

8.12 Users may not agree to a licence or download any material for which a registration fee is charged without first obtaining the written permission of a Director and informing the Head of IT.

### Frivolous/Wasteful/Inefficient use

8.13 Computer resources are not unlimited. Network bandwidth and storage capacity has finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others e.g. sending large files for invites to events at Look Ahead.

8.14 Frivolous use is a waste of Look Ahead's resources because the employee will not be performing their contractual duties during this time.

8.15 Any inappropriate overuse may amount to a breach of the policy.

8.16 Training is offered to all staff at Look Ahead to enable them to carry out their role. It is therefore important that they discuss and agree their training needs with their manager. Managers must assess their staff regularly and make staff aware of the IT training available, as well as staff highlighting their personal need for training.

### E-mail

8.17 Permitted use of internal e-mail and external e-mail is covered by Appendix 2.

### Internet

8.18 Permitted use of the Internet is covered by Appendix 3.

## 9 Hardware and Software Procurement

9.1 All IT equipment is to be purchased by the IT team to ensure the equipment is compatible with Look Ahead's IT system and that the correct licenses are in place, the IT Team is the sole authority for submitting requests for IT equipment & software for all Look Ahead schemes.

9.2 All IT related hardware and software will be specified by the IT team. Hardware and software cannot be purchased without a completed IT Capital Expenditure Form (CAPEX). This needs to be completed and signed by the requestor's line manager.

9.3 On receipt of the completed CAPEX form, the request will be actioned by a member of the IT Team and when ready for delivery the requestor will be notified.

9.4 The IT Team will, where necessary, amend the requirements based on compatibility with Look Ahead's infrastructure. You will be notified of any amendments to your order and the reasons for this.

9.5 All purchases of IT equipment and software will be ordered by the IT Team using approved suppliers.

# 10 Security

## System Access

10.1 It may be a criminal offence for an unauthorised person to attempt to access a system or information within systems or to attempt to exceed the computer facilities and privileges granted to them. Users committing an offence documented within the Computer Misuse Act 1990 may be disciplined as well as face civil and / or criminal action.

## Personal computer (PC) or terminal security

10.2 It is the responsibility of all PC and terminal users to take all reasonable precautions to safeguard their computer and the information contained upon it. This includes protecting it from physical hazards, including spilling liquids and not allowing unauthorised users to access the computer system, by leaving PCs logged onto the network whilst away from their desks for longer than a few minutes.

10.3 sers should lock their PC screens and use screensaver passwords if they are absent from their desks. Press Ctrl / Alt and Del keys together and select “Lock Workstation”. The screen will automatically lock after 15 minutes regardless.

10.4 Users must not under any circumstance use a PC if not logged into the network using their own login ID. Where a user leaves the building the PC should be logged off the network.

10.5 Users should save their work on a regular basis particularly when moving away from their desks. Power interruptions are commonplace in offices and work is often needlessly lost by not saving the document three or four times an hour.

10.6 Special consideration should be given to the protection of portable computers, as these are more open to theft and physical damage (e.g. being dropped).

10.7 Look Ahead’s insurance states that Portable Computers must not be left unattended in cars.

10.8 Sensitive information should not be stored on the hard disk of a portable computer unless it is a company supplied portable device or removable media with encryption technology installed.

10.9 At the end of each day or when offices are unoccupied any `confidential’ information must be locked away in pedestals, filing cabinets or offices as appropriate.

## Passwords

10.10 Users will be allocated a username and password to access the network and each application as applicable. These should not be recorded in any way that will enable access by another individual.

10.11 Users must not under any circumstance share logins or passwords.

10.12 Where possible all users should use a "Strong Password" which means a password that contains at least 6 characters; consists of a combination of upper and lower case letters, numbers and special characters. Users are prompted to change their password at least every 90 days.

10.13 All computer system users should choose passwords that cannot be guessed easily, such as "password", "welcome", etc. Passwords should not be related to the user's job or personal life. Passwords should not contain the user's first or last name or their login user ID.

10.14 Passwords should not be divulged to other individuals or third parties under any circumstances other than an authorised person. Even then, passwords should be disclosed in person (not over the phone or by e-mail) to a known, trusted source. If a password is compromised or you believe a password has been compromised, it should be changed as soon as possible. You must notify the IT Helpdesk of any password compromises.

## Unauthorised software

10.15 It is expressly forbidden for users to install software they have received from any source. This includes programs stored on floppy disk, CD-ROM, or downloaded via the Internet unless agreed by the Head of IT.

10.16 Look Ahead reserves the right to audit all personal computers or storage media on a regular basis and any user responsible for the use of unauthorised software amounts to a breach of the policy and potentially leading to appropriate action under Look Ahead's Disciplinary procedure.

10.17 Equipment will be ordered by the IT team according to workload. Where equipment or software is authorised and ordered an installation date will be scheduled, however this may change according to IT priorities.

## Virus detection

10.18 Files obtained from sources outside Look Ahead, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other on-line services; files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage Look Ahead's computer network.

10.19 Users should not download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Look Ahead sources, without first scanning the material with approved virus checking software.

10.20 If you suspect that a virus has been introduced into Look Ahead's network, notify the IT helpdesk immediately.

10.21 Look Ahead has firewalls and virus detection software installed and these are kept under regular review.

10.22 The virus checker must be allowed to run on a PC at the set time as it protects the Look Ahead network.

### Network Security

10.23 Within its own area of responsibility Look Ahead shall implement rigorous measures such as a "firewall" to protect against unauthorised accesses from external sources such as the Internet.

### Wireless Communications

10.24 It is strictly forbidden to install, use or access any wireless communication network without permission of the IT Department.

10.25 All wireless networks must utilise both appropriate encryption and authentication standards in order to mitigate the risk of unauthorised access as defined by the IT Team at the time at a minimum WPA2 with AES.

### Spam, Phishing and other Trojan attacks

10.26 IT will make all reasonable efforts to repel Spam and unwarranted email from reaching users mailboxes from external sources. However it is not possible to block all such emails. Some of the material contained in these email may be considered offensive. Look ahead has no control over the contents of such emails. If a user finds any material offensive they should contact the IT help desk with details of the incident.

10.27 Users should never open suspect emails, nor follow links, open attachments or run programs that are from non trusted sources. If in doubt they should contact the IT help desk.

10.28 The Look Ahead IT team will never request your username or password by email. You should never disclose this or any other details (including banking details) by email or on a non trusted website. It is users' responsibility to vet the validity of all sites or requests.

## 11 Personal Identifiable Data

11.1 Personal Identifiable Data (PID) must be kept secure and confidential at all times

11.2 Only persons with a legitimate relationship to the customer are allowed to view PID information.

11.3 PID must only be held in approved systems namely the Customer Information

11.4 Management System (CIMS), Genero, Document Management and secure data directories.

11.5 PID information should not be held in any other systems without the consent of the Head of IT.

11.6 Staff should make sure that whilst inputting PID it is not visible to unauthorised persons

11.7 In no circumstances should PID be stored on PC, Laptop or other portable device unless the device has encryption installed such as the company mobile working solution

11.8 All waste paper which has personal or confidential information or date on must be placed in confidential waste bins. Under NO circumstances should this type of waste paper be thrown away with normal rubbish in waste paper bins.

11.9 PID information is not to be sent using standard Email. PID can only be sent using the Look Ahead secure email system.

11.10 For additional guidance, refer to the Confidentiality and Data Protection policy

## 12 Security Incident Management

12.1 An incident relating to breaches of security and/or confidentiality could be anything from users of computer systems sharing passwords to a piece of paper identifying a customer being found in the high street.

12.2 A security incident might be a 'usual' everyday event, e.g. accidentally entering the wrong password or the wrong user id, forgetting to change a password within a specified time period or an 'unusual event e.g. something odd happening on a screen, a computer file disappearing, an unaccompanied unidentified stranger in a restricted area.

12.3 Hence, the potential impacts of security incidents can be wide ranging. Something that may initially appear to be an IT issue may in fact be something that has much wider implications, such as a break-in where equipment has been stolen that contains patient data or in which paper records were also removed.

12.4 An IT security incident is defined as any event that has resulted or could result in

- The disclosure of confidential information to any unauthorised person
- The integrity of the system or data being put at risk
- The availability of the system or information being put at risk
- Threat to personal safety or privacy
- Legal obligation or penalty
- Financial loss
- Disruption of activities
- Failure to meet statutory laws and regulations

12.5 All incidents must be reported to the IT Helpdesk.

12.6 A security event may be identified through a variety of means, however ultimately it is important that the event, if related to IT, is reported with the IT Help desk. As with any IT incident, the IT Help desk need to be aware of and log each and every IT security incident and should be a single point of knowledge regarding the status of IT incidents.

12.7 If you suspect that an information security event is in progress or may have occurred – particularly one which may cause substantial loss or damage you

should *immediately* notify the IT Helpdesk and submit an information security event report form (available from the IT Help desk.).

12.8 Incidents should be classified according to the severity of the risk, as follows:

- **High risk** of harm to customers, staff and members of the public whose confidentiality has been breached.
- **Intermediate** risk of harm to customers, staff and members of the public whose confidentiality has been breached
- **Low risk** of harm to customer, staff and members of the public whose confidentiality has been breached.

12.9 The IT Help desk will then undertake the First Assessment. Should it be necessary to undertake a second assessment, this will be undertaken by the Head of IT.

12.10 Any employee or agent who becomes aware of errors that may have been made by the information system(s) must formally report such errors to their line manager and to the IT Help Desk. The seriousness of an error is not the main issue; even minor errors may be symptomatic of a deeper and much more serious issue.

# 13 Physical Security

13.1 All computer and related equipment shall, where practical be located in secure lockable cabinets and racks. Suitable access controls should be in place, these may be:

- Lockable doors
- Keypads
- Fob or Biometric access control

13.2 Access to the Look Ahead computer rooms is strictly limited to Look Ahead IT staff, Management and authorised contractors.

# 14 Equipment Security

## Equipment Siting and Protection

14.1 IT equipment will be purchased by, installed and sited in accordance with the manufacturer's specification. Equipment must always be installed by, or with the permission of the IT team.

14.2 Drinking and eating is not permitted in areas housing computer equipment.

## Equipment Maintenance

14.3 All central equipment including file servers and network components will be covered by third party maintenance agreements.

14.4 All such third parties will be required to sign confidentiality agreements. Records of all faults or suspected faults will be recorded by the IT team.

# 15 Backups and Business Continuity

## Network

15.1 The IT Team is responsible for taking and securing system(s) back-ups for all data and software relevant to the systems that are controlled centrally. Look Ahead employs an off-site tape storage company to secure and administer data tapes.

15.2 Users who have other software and data shall be responsible for their own back-ups and, in the interest of Look Ahead they should ensure that this is done properly on a regular and routine basis.

## Local PCs

15.3 Where possible users should save all files on a network drive (i.e. not on the C: drive or floppy disks) to ensure that adequate backups are taken and there is a minimal risk to Look Ahead data. If work is stored on a local PC there should be a backup made to a network drive for essential files.

## Business Continuity

15.4 The IT Team has devised an IT Disaster Recovery (DR) plan that is incorporated into the organisational Business Continuity plan. An IT DR site has been setup in a secure off-site data centre. All critical corporate and customer data is replicated in real-time to prevent data loss.

# 16 Remote Access

## Staff Remote Access & Home Workers

16.1 All devices must use secure passwords to prevent unauthorised access to information stored on the computer.

16.2 All devices using a remote access connection to connect to the Look Ahead network must have up to date Anti-Virus and Spyware software installed.

16.3 Only authorised users are permitted to access network resources.

16.4 If you work at home or off-site then you are directly responsible for the security of the information and equipment that you use.

16.5 If you use a non-Look Ahead supplied personal computer or laptop you must ensure it has up to date Malware protection and any relevant security Patches to the systems and or software.

16.6 It is you responsibility to store data on the central systems where they will be backed up and secure. You should not store data on the local storage of your mobile device (e.g. laptop hard drive)

16.7 The downloading/uploading of application software is strictly prohibited

16.8 Allowing non-authorised persons to access information/services via remote access is strictly prohibited.

16.9 Ensure all devices are locked way when left unattended.

16.10 Employees are not permitted to download any company information to a Home Computer or removable media.

### Third Party Remote Access

16.11 Any 3rd Party being a supplier, client, external company or external consultant before being granted access to the Look Ahead network will have to provide a business case and to have obtained authorisation to connect.

16.12 The 3rd Party will be required to verify they conform to the Look Ahead IT policy and to sign to this effect.

16.13 All 3rd Parties will only view /access data that is required to complete their contractual obligations.

16.14 All data is to be treated as confidential and 3rd parties are to sign a Look Ahead confidentiality agreement prior to accessing data.

16.15 Look Ahead reserve the right to withdraw remote access without notice to any 3rd Party. Where this presents a breech in the ability to deliver to contract the terms of that contract shall abide.

## 17 Asset Management

### General

17.1 IT equipment is assigned to the position, not the individual, and remains with the position if the individual terminates employment or is transferred to another position.

17.2 All contract managers and team leaders are required to have a complete asset register locally of all portable IT equipment such as netbooks, dongles, signature pads, laptops , mobile phones and tablets.

17.3 The asset register should indicate which member of staff each device is allocated to. The register should be available on request to ensure the organisation keeps track of all assets.

17.4 Acquisition of IT equipment shall follow a central purchasing method. Purchases, contracts, amendments and renewals will be processed through the Head of IT or designee.

17.5 All assets are to be signed out electronically by the staff member allocated the assets.

17.6 Assets are not to be given to other staff members without being recorded in the local asset register and with IT.

17.7 Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

### Disposal

17.8 Look Ahead assets have a pre-defined life-span determined by the Head of IT. All assets to be disposed must be marked inactive within the asset management system and a record kept of date of disposal.

17.9 For the purpose of this policy, IT Equipment is defined as computer terminals, PC system units, printers, monitors, modems and network equipment.

17.10 Circumstances for authorised destruction are:

- The equipment is beyond reasonable repair
- It's cheaper than disposal
- The item has no capital value

17.11 In all cases the Financial Standing Orders will prevail over disposal of redundant equipment.

17.12 Authority to dispose of IT equipment must be obtained from the Head of IT (after reasonable efforts have been taken to see if any other departments are able to use the equipment) as per standing orders.

17.13 Old PCs and any removable media with licensed software stored on them must have this removed before disposal to avoid software license infringement. Also any data that is stored on for example the hard drive, must be removed to keep sensitive data secure.

17.14 If a 3rd Party is used to dispose of IT assets, a certificate of destruction must be obtained and kept for audit purposes.

## 18 Exceptions

18.1 The Head of IT is responsible for reviewing and approving exceptions to IT policies.

18.2 The Head of IT may grant exceptions to this policy under extraordinary circumstances. Requests for exceptions must be made in writing to Head of IT stating the business need and unique circumstances requiring an exception.

18.3 The Head of IT will evaluate and determine if the requested exception can be reasonably resolved through technology within the confines of the company's technology environment.

18.4 For granted exceptions, the requester must establish with the Head of IT a plan for technical support, training, and maintenance. The plan shall be developed prior to purchase or implementation of non-standard technology.

## 19 Monitoring of Computer Usage

19.1 Look Ahead will randomly monitor e-mails and Internet use and other aspects of its computer system periodically to prevent abuse of the system and breaches of this policy. Where abuse is suspected it will be specifically monitored.

19.2 This may include, but is not limited to, monitoring internet sites visited by users, monitoring of time spent on the Internet, monitoring volume of e-mail traffic, monitoring file downloads, and specific communications sent and received by users when appropriate.

19.3 Look Ahead will follow defined procedures in carrying out any monitoring, which complies with relevant legal requirements and / or good practice.

## 20 Privacy

20.1 Employees are provided with computers to enable them to perform their jobs.

20.2 Users waive rights of privacy in anything they create, store, send or receive using Look Ahead's computer equipment or Internet access where Look Ahead has reason to investigate.

20.3 By using Look Ahead's computer system users consent to allow Look Ahead authorised personnel access to and review of all materials created, stored, sent or received by the user through any Look Ahead network or Internet connection in accordance with defined procedures.

## 21 Home and Personal Computers

21.1 Look Ahead does not provide free support for personal computers or related items, except where they are used for Look Ahead business and remote access.

21.2 Look Ahead will not be responsible or liable for any home PC repair arising from or after access to the Look Ahead network unless the hardware is an asset of Look Ahead. Access to the Look Ahead network on staff PCs are at the users own risk.

## 22 New User Request Form

22.1 A new user request form must be completed by user's line managers to ensure the appropriate level of access is given commensurate with the job position held. **(Appendix 4)**.

22.2 This is to be sent to the IT Helpdesk. Managers should allow 5 working days before the user starts with Look Ahead in accordance with the IT Service Level Agreement.

## 23 Change of User Access Form

23.1 Changes in user access levels must be completed on a Change of User Access form by the user's line manager and 5 working days before the change is required in accordance with the IT Service Level Agreement. **(Appendix 5).**

## 24 Leavers Form

24.1 When a user leaves the employ of Look Ahead a Leaver's Form must be completed by the user's line manager and 5 working days before the change is required in accordance with the IT Service Level Agreement. **(Appendix 6).**

## 25 Data Protection Act

25.1 Look Ahead staff and agents should adhere to current Data Protection legislation and practice. Where doubt exists they should contact the nominated Data Protection officer or the Head of IT for guidance.

## 26 Summary Document

26.1 A summary of this policy is produced for managers to issue to temporary/agency workers. This is attached as Appendix 8.

## 27 Equality and Diversity

27.1 Look Ahead is committed to Equality, Diversity and Human Rights.

27.2 We are committed to helping customers to access information about their homes and services in a way that suits individual needs.

27.3 If any person believes that they have not been treated in accordance with this policy, or they are unhappy about anything related to the policy, they may complain in accordance with our Feedback and Complaints Policy.

## Appendix 1 (Network Access Form)

ALL USERS ARE REQUIRED TO COMPLY WITH LOOK AHEAD'S INFORMATION SECURITY POLICY. ANY MISUSE MAY AMOUNT TO A BREACH OF THE POLICY AND POTENTIALLY LEAD TO APPROPRIATE ACTION

By signing this form the user is agreeing to have read and understood the contents of this policy document.

Job Title: _____

Name of Post Holder: _____

Signed by Post Holder: _____

Date: _____

(Original to be filed with HR on Personnel file / copy to be filed on IT Computer security file by the IT Team)

**All users must comply with Look Ahead's Data Protection Policy and the Data Protection Act 1998.**

| **For the use of HR only** | **For use of IT only** |
|---|---|
| Date Received | User ID: |
| By whom | Date account setup |
| Scheme/Project Name | By whom |
| Scheme/Project Manager | Date to be enabled |
| Start date if known | By whom |

# Appendix 2 (Internal and External Email Policy)

## 28 Permitted Use of E-mail

28.1 Most Look Ahead staff are entitled to use an individually allocated Look Ahead e-mail facility.

28.2 All users have a responsibility to use Look Ahead's computer resources in a professional, lawful and ethical manner and in accordance with procedures, the Data Protection Act (Appendix 7) and Harassment Policy.

### E-mail Use Limitations

28.3 Do not write anything in an e-mail that you would not be prepared to say to the recipient in person. Avoid the use of words, phrases and language that the recipient may find offensive. Comments in e-mail relating to third parties must not make unfounded claims about activities or abilities. Users must not send racist, sexist, pornographic, abusive or defamatory messages via e-mail. Users should be generally sensitive to the use of inappropriate language. Look Ahead's Harassment Policy should be considered whilst communicating using e-mail. Also avoid the use of capitals and excessive bold font since this can convey an aggressive tone to the communication. Do not send unsolicited e-mails under any circumstance as this contravenes the Communications Act 2003.

28.4 Avoid sending 'highly' confidential or sensitive information by e-mail. All attachments received by e-mail must be scanned using approved anti-virus software.

28.5 Staff and agents are reminded that email and other electronic documents can be legally binding. Therefore the same care and governance must be exercised around making contractual commitment on behalf of Look Ahead through these media as traditional methods. At all times Standing Orders must be adhered to.

28.6 E-mails are not always guaranteed to arrive and staff are encouraged to also use paper based methods if the matter is significant. Staff could also flag the message so that they are advised when the message has been read.

28.7 It is important to keep copies of e-mails where e-mails are used in the course of correspondence on operational matters; these paper based records may become important evidence (e.g. if matters arise about the formation of a contract).

28.8 It is important for staff to check the contents or attachments of e-mails before they are forwarded.

28.9 Disclaimers are automatically attached to e-mails. Staff must not attempt to remove the disclaimer.

28.10 Staff are reminded not to use Look Ahead email for personal or non Look Ahead related correspondence. This includes registration to mailing lists, notification services etc.

28.11 Staff should not promote or provide your own or other Look Ahead email addresses to any third party not directly related to your specific role and activity.

## Communication of Look Ahead information

28.12 Unless expressly authorised to do so, users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or confidential information belonging to Look Ahead. Unauthorised dissemination of such material may result in disciplinary action as well as civil and / or criminal action.

## Frivolous / wasteful /inefficient use

28.13 These acts include, but are not limited to:-

- Sending mass mailings or chain letters by e-mail.
- On-going exchange of e-mails which are inappropriate in length / frequency for the purpose to which they refer
- Maintaining hundreds of e-mails in your 'In box' and 'sent items' folder

28.14 In addition, users are expected to manage their e-mails effectively to avoid unnecessary use of valuable storage space. Ideally users should maintain less than 100 e-mails in their 'In box' and 'sent items' folder with e-mails you wish to retain being archived.

## External Email

28.15 The provision of external email has been established for business purposes and should be used accordingly.

28.16 Personal emergency / urgent emails that cannot be sent out of working hours are acceptable.

28.17 Non-urgent emails should be sent during the employee's own time, and should be kept brief and to a minimum.

28.18 There is an electronic log created containing details of the sender and recipient of all external email, which is monitored by the Head of IT in accordance with defined procedures.

# Appendix 3 (Internet Policy)

## 30 Permitted Use of the Internet

30.1 Some Look Ahead staff are granted access to the Internet for business purposes. This facility is provided to support activities pursuant to Look Ahead's business activities. Internet access may be withdrawn temporarily or permanently without notice to one or more individuals without explanation.

30.2 The use of the Internet for non work related activities is strongly discouraged, however Look Ahead recognise that staff may occasionally use this resource for personal reasons. Any personal use must be within reasonable constraints for example during designated lunch breaks or to deal with a personal emergency.

30.3 The Internet is outside Look Ahead's control so it should not be relied on to complete a task or deliverable.

30.4 All users have a responsibility to use Look Ahead's computer resources in a professional, lawful and ethical manner and in accordance with procedures and the Data Protection Act (Appendix 7).

### Internet use limitations

30.5 Staff and agents are reminded that email and other electronic documents can be legally binding. Therefore the same care and governance must be exercised around making contractual commitment on behalf of Look Ahead through these media as traditional methods. At all times Standing Orders must be adhered to.

30.6 Staff and agents should never use this resource for any business related activity not directly associated with or sanctioned by Look Ahead.

30.7 Users should only subscribe to appropriate and necessary mailing lists. These should be prior approved by their Line manager. On-line chat capability should only be used for legitimate business purposes.

30.8 Particular care should be exercise in the use of social networking sites. Users are reminded of the policies and restrictions in this document (eg libellous statements, defamatory remarks). It is important to remember that you should not attempt to represent Look Ahead or your professional capacity in any online correspondence. The use of Social Network sites is strongly discouraged.

### Accessing the Internet

30.9 To ensure security and avoid the spread of viruses, users accessing the Internet through a computer attached to Look Ahead's network must do so through an approved Internet firewall or other security device.

30.10 Bypassing Look Ahead's computer network security by accessing the Internet directly by modem or other means is strictly prohibited, unless with prior agreement from the Head of IT.

## Logging internet use

30.11 Look Ahead may monitor and log internet use from its systems. This may identify a specific workstation and or individual user, time spent, sites visited or other information. These logs may be used to identify inappropriate behaviour, traffic volumes or other information. Any such logs are solely for Look Ahead's use.

## Frivolous / wasteful / inefficient use

30.12 Use of the internet for any purpose should not interfere with an individual's ability to deliver their workload.

30.13 These acts include, but are not limited to, spending excessive amounts of time on the Internet, playing games, uploading or downloading large files, accessing streaming audio and or video files, or otherwise creating unnecessary loads on network traffic associated with non-business related use of the Internet.

## Blocking sites with inappropriate content

30.14 Look Ahead has the right to utilise software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed as inappropriate in the workplace.

30.15 Look Ahead or its service providers reserve the right to block any site, protocol, or service at its discretion without notification or explanation regardless of the site content.

## Illegal copying

30.16 Users may not illegally copy material protected under copyright law or make that material available to others for copying.

30.17 Users are responsible for complying with copyright law and applicable licence agreements that may apply to software, files, graphics, documents, messages, and any other material to be downloaded or copied.

30.18 Users may not agree to a licence or download any material for which a registration fee is charged without first obtaining the written permission of a Director and informing the Head of IT.

## Disclaimer

30.19 The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. It is an employee's duty not to look at, or in any way process, such material even if it comes up accidentally on a search. For the purpose of clarity, viewing or downloading obscene material is inappropriate use.

30.20 Look Ahead would not normally take action against employees who have offensive, obscene or sexually explicit or any other inappropriate material sent to them without soliciting it, but employees should be aware that the introduction of such material onto Look Ahead's network will be dealt with. On receipt of such material, staff should ensure it is promptly deleted – the

IT team must be notified of this event. Failure to do so amounts to a breach of the policy and may potentially lead to appropriate action under Look Ahead's Disciplinary procedure.

30.21 Users who disclose personal information on the network should be aware that it will be saved as part of the network back up.

## Appendix 4 (New User Request Form)

You are required to complete the following form to ensure that all new staff in your department have the appropriate access to Look Ahead's IT systems to enable them to fulfil their duties.
Users will be provided with standard network access including a home directory, use of internal e-mail, Word and Excel. Other applications must be requested below.
Please ensure that you provide the IT Team with at least 5 working days notice to set up new accounts before the new employees start date.
Please note you should always use the most current forms. Please check the IT Section of the Look Ahead Intranet for updated versions of this document.

## IT New Starter Form

Forms that are not completed correctly will be returned to the sender.

Please note: some fields may not apply to your new staff member, please leave these blank.

**Requestor Details**

| |
|---|
| Requestor name - |
| Requestor job title **(OM, CM, Manager, Team Leader)** - |
| Requestor location - |

**New Starter Details**

| |
|---|
| New starter name - |
| New starter job title - |
| New starter location - |
| Employment status **(permanent, agency, volunteer, PSA)** - |
| Start date - |
| End date - |
| Network usage policy form sign-off with HR (yes / no) - |

**Network / E-mail Access Details**

| |
|---|
| Specific G: drive folders **(folder names please)** - |
| Archived data required for **(name of ex-staff member please)** - |
| Add to e-mail distribution lists **(list names please)** - |
| Access to shared mailboxes **(mailbox names please)** - |

**Genero Access Details**

| |
|---|
| Copy permissions from **(name or user-id for existing staff member)** - |
| Specific tasks **(e.g. taking rents, cash batches, e.t.c)** - |
| For Hostels, state the Supported Housing Scheme Indentifier - |
| Preferred Printer(s) **(Genero print queue number please)** - |

**Cisco Telephony Details**

| |
|---|
| Is there a preferred extension we should provide **(ext. number. please)** - |
| Is voicemail required **(yes / no)** - |
| Is a "line 2" required **(please provide the ext. number)** - |

**CIMS Access Details**

| |
|---|
| Access Level **(service person, deputy manager, manager, administrator)** - |
| Number of hours to be worked per week - |
| Will user be working at more that one service **(service names please)** – |

| |
|---|
| **Additional requirements** - |

## Appendix 5 (Change of User Access Form)

You are required to complete the change of User Access form when there is a change of access requirements for staff within your department to ensure that employees always have the appropriate level of access to Look Ahead's IT systems to enable them to fulfil their duties. Please ensure that you provide the IT Team with at least 5 working days notice of any changes to existing user accounts and indicate the date when the changes should come into force.
The change of access form is electronic and should be submitted by email to helpdesk@lookahead.org.uk. It is available on the intranet under the IT section. Please contact the helpdesk on 020 73684635 if you require assistance with this.

Please note you should always use the most current forms. Please check the IT Section of the Look Ahead Intranet for updated versions of this document.

| | | | | |
|---|---|---|---|---|
| **Requestor** | This section is for the details of the line manager making the access request.<br>Please complete all details. | | | |
| **Forename** | **Surname** | | | |
| **Position** | | | | |
| **Location** | | | | |
| **Tel No.** | **Extension No.** | | | |
| **User Details** | Please complete all details. | | | |
| **Forename** | **Surname** | | | |
| **Title** | | | | |
| **Department** | **Location** | | | |
| **Tel No.** | **Date to Activate** | | | |
| **New Access Requirements** | Please select only the **newly required** applications. | | | |
| **Genero** ☐<br>**Ext E-Mail** ☐ | **CIMS** ☐<br>**Internet** ☐ | **SUN** ☐ | **PWA** ☐ | **Snap** ☐ |
| **Specific Requirements** | Please indicate any special requirements such as access to applications not listed above or specific folders/directories. | | | |
| | | | | |
| **Deleted Access Requirements** | Please select only the applications where access is no longer required. | | | |
| **Genero** ☐<br>**Ext E-Mail** ☐ | **CIMS** ☐<br>**Internet** ☐ | **SUN** ☐ | **PWA** ☐ | **Snap** ☐ |
| **Specific Requirements** | Please indicate any previous special requirements including access to applications or specific folders/directories to be removed/disabled. | | | |

## Appendix 6 (Leaver's Form)

You are required to complete this form if your are the line manager of a member of staff with access to Look Ahead's IT systems when they leave the organisation.

It is important that you consider whether there is any need to retain any of the user's files or e-mails. You should also consider whether their e-mail address should be disabled immediately they leave Look Ahead, or set up with an auto response or forward to another individual for a short period of time, typically one month.

Please note you should always use the most current forms. Please check the IT Section of the Look Ahead Intranet for updated versions of this document.

**IT Support Team - Leaver Notification Form**
Please read the "notes for use document" before completing this form.
Forms that are not completed correctly will be returned to the sender.

**Requestor Details**

| |
|---|
| Requestor name - |
| Requestor title - |
| Requestor location - |

**Leaver Details**

| |
|---|
| Leaver name - |
| Leaver title - |
| Leaver location - |
| Last Working Day (dd/mm/yy) - |

**Access to Archived Network / E-mail Data**

| |
|---|
| 'My Documents' folder access required? (type names) - |
| Archived e-mail data access required? (type names) - |
| E-mail forwarding required? (type names) - |
| 'Out of Office' message required? (type text) - |

**Cisco Telephony Forwarding & Voicemail Access**

| |
|---|
| Cisco extension forwarding required? (type number ) - |
| Voicemail message required? (type message) - |
| Access to voice mailbox required? (type names) - |
| **Additional requirements** - |

Return the completed form by e-mail to **Help Desk** on helpdesk@lookahead.org.uk

## Appendix 7 (Data Protection Act)

The 8 principles of the Data Protection Act are as follows:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

   These schedules can be found through the link http://www.dataprotection.gov.uk/dpr/dpdoc.nsf and follow the links.

2. 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.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. 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.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

   Look Ahead has a detailed Data Protection Policy which staff are required to understand and adhere to.

More detail about the Data Protection Act can be obtained from http://www.dataprotection.gov.uk/dpr/dpdoc.nsf

## Appendix 8 (Information Security Policy – Summary)

This summary of the Information Security policy and procedure is designed to make you aware of the main points of this policy in a clear and brief format so that you are able to understand its requirements and therefore be able to comply. If you have any queries you should refer to the full policy document. Should you still need clarification of any points within this policy then please refer to your line manager or the Head of IT.

### Main Policy Contents

### General

- All staff, including short term temporary and contract staff, with access to Look Ahead's computer systems are required to comply with this policy and new users will be required to sign a Declaration form (Appendix 1) which acts as an acknowledgement that the full policy has been read and understood.
- Any breach of this policy by an individual will be investigated under Look Ahead's disciplinary procedure.
- Users are provided access to computers and the network to assist them in the performance of their jobs and must use the resources in a professional, lawful and ethical manner and in accordance with procedures and the Data Protection Act 1998.
- Personal use, which should be within the employee's, own time is also governed by this policy. Personal use of the computer is a privilege that can be revoked at any time. An employee's own time is deemed to be their lunch break or outside normal working hours.
- All data created is the property of Look Ahead not the individual. The individual has no rights over data, ideas or other intellectual property developed created or stored on Look Ahead systems.
- Systems may be taken out of use for individuals or groups for example for maintenance. This should not provide reason for non delivery of business objectives. Should a user feel that system 'down time' is adversely affecting their ability to deliver work to time they should raise the issue with the IT helpdesk who may consult with their line manager
- Look Ahead reserve the right to restrict or deny access to any individual or group without prior notification or giving justification (for example in a suspected security breech). Should this adversely affect a user's ability to perform their role they should in the first instance contact the IT Helpdesk and their Line Manager for assistance.

### Usage Limitations

- Look Ahead's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code or any other prejudicial materials.
- Under no circumstances should the computer network be used to send any defamatory, obscene or discriminatory material and / or any use of the e-mail system to harass members of staff in any way.
- Users may not illegally copy or download material protected under copyright law or copy / download software, files, graphics, documents, messages or any other material that may infringe applicable licence agreements.
- Users may not download or attempt to copy any software on to the network or a PC under any circumstances without the prior agreement of the Head of Information Systems.

- Users may not agree to a licence or download any material for which a registration fee is charged without the written permission of a Director.
- The user must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others.
- E-mail must not be used to i) send highly confidential or sensitive information, ii) as a communication medium for contractual commitment, iii) distribute propriety information, data, trade secrets or confidential information belonging to Look Ahead, iv) send racist, sexist, pornographic, abusive or defamatory messages.
- Under no circumstances should unsolicited e-mails be sent as this contravenes the Communications Act 2003.
- E-mail is made available for business use and should only be used for personal use in unavoidable circumstances, during the employees own time and with prior agreement with your line manager.

**E-mail**

- Do not write anything in an e-mail that you would not be prepared to say to the recipient in person or use words, phrases and language that the recipient may find offensive.
- Do not send racist, sexist, pornographic, abusive or defamatory messages via e-mail or unsolicited e-mails.
- Do not send 'highly' confidential or sensitive information or use e-mail as a communication medium where any contractual commitment is made or received.
- Staff must not remove the automatically attached e-mail disclaimers.
- Users are expected to manage their e-mails effectively so that unnecessary storage space is not used.
- The provision of external e-mail has been established for business purposes and should be used accordingly.

**Internet**

- Users must not under any circumstances engage in on-line chat rooms.
- Users must not use the Internet to: play games, upload or download large files, access streaming audio or video files or upload/download software of any description unless through prior agreement with the IT Team.
- Look Ahead has the right and may use software to identify and block access to Internet sites containing material deemed inappropriate in the workplace.
- The Internet must not be used as a communication medium where any contractual commitment is made or received on behalf of Look Ahead.
- This policy governs the use of the Internet for private use, which should be minimal and in the employee's own time. The employee's own time is deemed to be their lunch break or outside working hours.
- Where an employee is authorised to access Look Ahead systems or Data remotely they must take all reasonable precautions to protect from stolen passwords, virus attack or other threats to the system from the device or system they are using to access Look Ahead.

**Security**

- It may be a criminal offence for an unauthorised person to attempt to access a system or information within systems or to exceed the computer facilities and privileges granted to them.

- Users must take all reasonable precautions to safeguard their computer and the information contained upon it.
- Users must not leave their PC's logged onto the network whilst away from their desks for longer than a few minutes and should always be logged off when leaving the building. As an additional measure users should use screensaver locks/passwords.
- Portable Computers must not be left unattended in cars or sensitive information stored on the hard disk under any circumstances.
- Data Keys or other mobile storage media should never be left unattended. All unnecessary data should be wiped from the device when not needed. Encryption and other measures to protect the data should be exercised for sensitive information.
- Passwords should not be recorded or in any way divulged which would enable access by another individual. Users must not share logins or use a PC if not logged in as them self. If you know or believe a password has been compromised it should be reported immediately to the IT helpdesk and changed as soon as possible.
- All computer users should choose passwords that cannot be easily guessed, are not related to the user's job or personal life. A 'Strong Password' must be used where possible. A 'Strong Password' is one that contains at least six characters, which consists of a combination of upper and lower case letters, numbers, and special characters.
- It is forbidden for users to install software they have received from any source unless agreed by the Head of Information Systems.
- Look Ahead reserves the right to audit all personal computers, email, and files on a regular basis.
- Users should not download files from the Internet, accept e-mail attachments from outsiders, or use disks from non Look Ahead sources, without first scanning the material with approved virus checking software. A number of measures are in place to automatically scan e-mails and their attachments and therefore the virus checker must be allowed to run on a PC at the set time as it protects the Look Ahead network.

**Backups**

- Backups of the Look Ahead servers take place centrally. Where possible users should save all files on a network drive to ensure that adequate backups are taken. If work is stored on a local PC users should ensure that a backup is made to a network drive of essential files.

**Monitoring of Computer Usage**

- Look Ahead will randomly monitor all aspects of its computer system to prevent abuse and breaches of this policy. Monitoring will include, but is not limited to, monitoring internet sites visited by users, time spent on the Internet, e-mail traffic, file downloads and specific communications sent and received by users when appropriate.

**Privacy**

- Users waive rights of privacy in anything they create, store, send or receive using Look Ahead's computer equipment or Internet access where Look Ahead has reason to investigate. Users also consent to allow Look Ahead authorised personnel access to and review of all materials created, stored, sent or received by the user.

## Version Control

| | | | |
|---|---|---|---|
| **Version no.** | 2 | **Date effective:** | August 2016 |
| **Brief summary of changes:** | | New template | |
| **Colleague consultation:** | | N/A | |
| **Customers consulted:** | | N/A | |
| **Results customer consultation:** | | N/A | |
| **Other consultation:** | | N/A | |
| **Signed off by:** | | N/A | |
| **Author:** | | N/A | |
| **Review date:** | | N/A | |


King's Building
16 Smith Square
London SW1P 3HQ

Tel: 020 7937 1166
policyresponse@lookahead.org.uk

**lookahead.org.uk**

Services we would be proud
for our loved ones to receive