Data Protection and Confidentiality

Policy and Procedure

Policy Author: Claire Luxton, Head of Information Governance and Assurance
Valid From: May 2018
Review due: May 2023

King's Building
16 Smith Square
London SW1P 3HQ

T: 020 7368 4600
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

1 Scope 6
2 Introduction 6
3 Responsibilities 6
4 Lawfulness of Data Processing 7
Legal Basis for processing information 7
Special categories 8
5 Processing of Data 9
Personal data 9
Sensitive personal data 9
Criminal convictions & offences 10
Access rights 10
Customers access to personal files 10
Employee access to personal files 11
Sharing of customer information 11
6 Disclosure of information to a third party 11
7 Exemption from disclosure of information 12
8 Storage 12
Storage of customer files (paper records) within staffed offices 12
Electronic records (storage) 12
Electronic records (retention) 12
Use of portable equipment 12
Use of email 13
Email encryption 13
Printing 13
Taking documents outside of staffed services or offices 13
9 Displaying Retention Information 14
10 Archiving, Retention Periods, and the disposal of Records 14
Archiving 14
Retention periods 14
Disposal of paper records 14
Disposal of electronic records 15
11 Data and Security Breaches 15
Evaluate and respond 15
14 Closed Circuit Television (CCTV) 16
12 Visitors Logs in Services 16
Visitors logs and storing copies of ID 16

12 Data Handling Training 16
Appendix 1: Staff Procedure 17
Files and Data held on Employees 17
Personal records 17
Training record 17
Appraisal and supervision records 17
Recruitment records 18
Payroll records 18
Appendix 2: Consent Form 19
Appendix 3: Data Breach Reporting Form 22
Related Document 24
Version control 25

Policy

1 Scope

1.1 This policy and procedure applies to all Look Ahead customers living within our supported and unsupported accommodation and supported by our staff. This also applies to all Look Ahead employees.

1.2 This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations (GDPR) 2016 and Data Protection Action (DPA) 2018 and any other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files, electronically, CCTV footage and photos.

2 Introduction

2.1 Look Ahead holds and processes information about its customers, employees and suppliers and under the legislations we are legally obliged to protect that information by ensuring:

- Data collection is fair and lawful and we must be open and transparent as to how the data will be used.
- Data can only be collected for a specific purpose.
- Any data collected must be necessary and not excessive for its purpose.
- The data we hold must be accurate and kept up to date.
- We cannot store data longer than necessary.
- The data we hold must be kept safe and secure.

2.2 The following document therefore sets out how we intend to meet these commitments, however it is important that each service is also familiar with the policies and procedures held by their local authority as well as any guidance from the Information Commissioner.

2.3 Look Ahead will ensure accountability and transparency in all our use of personal data and will comply with each of the principles as set out in 2.1.

2.4 **Look Ahead** is the data **controller** of the data we hold. We must maintain our appropriate registration with the Information Commissioners Office (ICO) in order to continue lawfully controlling (and/or) processing data.

3 Role and Responsibilities

3.1 The Head of Information Governance and Assurance on behalf of the CEO will have overall responsibility for ensuring that the organisation complies with its legal obligations.

3.2 The Information Governance Manager will be responsible for:

- Reviewing Data Protection and related policies.
- Advising other staff on tricky Data Protection issues.
- Ensuring that Data Protection induction and training takes place.
- Notification to the ICO.
- Handling subject access request.
- Approving unusual or controversial disclosures of personal data.
- Approving contracts with Data Processors.

3.3 Head of IT will be responsible for monitoring and overseeing that IT is compliance with the legislations.

3.4 All employees, volunteers and apprentices should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (Where 'employees' is used, this includes paid employees, volunteers, apprentices and PSA workers).

4 Lawfulness of Data Processing

Legal basis for processing information

4.1 Look Ahead will establish a lawful basis for processing data and that any data we are responsible for managing has a written lawful basis. Under GDPR At least one of the following lawful basis must apply whenever we process personal data:

- **Consent** - We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
- **Contract** - The processing is necessary to fulfil or prepare a contract for the individual.
- **Legal Obligation** - We have a legal obligation to process the data (excluding a contract).
- **Vital Interests** - Processing the data is necessary to protect a person's life or in a medical situation.
- **Public Function** - Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
- **Legitimate Interest** – Processing is necessary for the legitimate interest of the organisation.

4.2 The lawful processing basis under GDPR, which should cover most of the processing done by Look Ahead will comply with a number of **Legal obligations** under (*Article 6)(c), processing is necessary for compliance with a legal obligation to which the controller is subject.*

4.3 The legal basis of the processing for which personal data will be used as set out in the tenancy / licence agreement and any associated activity such as (but not limited to), sharing with local authorities and other support agencies, third party contractors, government agencies to assist with activities connected with tenancy agreement.

4.4 Look Ahead will also ensure that we fulfil our legal and regulatory obligations in providing care and support services, for example under the:

- Care Act 2014.
- Health and Social Care Act 2008 (regulated activities) Regulations 2014
- Mental Capacity Act 2005
- Mental Health Act 1983
- Housing Act 2004
- Homelessness Act 2002
- Homelessness Reduction Act
- Children's Act 2004
- Caldicott Principles
- (This is not an exhaustive list)

4.5 We must also comply with the Care Quality Commissions (CQC) standards for quality and safety.

4.6 Under legal obligation processing employee data is necessary for payroll and HR reasons including sick leave and other types of leave for which statutory payments are available. Also for the exercise or defence of legal claims, as well as complying with health and safety law in certain circumstances.

4.7 HM Revenue & Customs (HMRC) have a requirement on employers to record and retain certain personal information from a current and historic aspect and these legal requirements supersede an individual's request for deletion or change where that information is being processed and kept for those legal reasons.

4.8 There maybe some processing which may not comply with the legal obligation. The law allows us to also process data if it is in our **Legitimate Interests**, but we can only do this:

- If it does not affect the interests and fundamental rights of customer and employees and it does not override those interests.
- It does not have significant harm if data is breached or is intrusive.

4.9 The Law states that we must inform the data subjects of what we consider our legitimate interest would be. Our Legitimate Interest would be:

- To ensure that our services meet the needs of our customers
- To ensure we make use of our resources for our customers and employees and understand how we are performing
- To ensure we provide a safe service and
- To ensure we understand our customer's and employee's experiences through feedback and surveys

Assuming that the processing does not give rise to significant data security concerns or risk of harm to the customers or employees. In our view Look Ahead may lawfully process the customer's / employees data for these sort of purposes because Look Ahead or the relevant third party has a legitimate interest in carrying our that processing.

Special categories

4.10 Processing of special categories of personal data must be a lawful processing condition in addition to the lawful processing of standard personal data. Under GDPR, Article 9, the conditions that would apply to Look Ahead for processing special categories are:

- Protection of the vital interests of the data subject or another person where the data subject is legally or physically incapable of giving consent.
- Legal obligation on the controller in respect of employment, social security etc.
- Necessary for the purposes of preventative or occupational medicine, assessment of working capacity, medical diagnosis, provision of health or social care or treatment or the management of health and social care.

4.11 In most cases one of the conditions under special categories will apply. When replying on those conditions Look Ahead should avoid suggesting that it is also asking for the data subjects (customer/employee) consent.

4.12 In extreme circumstances where none of theses conditions apply, then Look Ahead must obtain explicit consent to the processing of special categories. Where consent is being relied on upon Look Ahead must ensure that consent is truly and freely given.

4.13 The consent must also be written in plain English and must be clear to understand. Customer and employees must also be made aware of their rights to withdraw consent.

4.14 A customer version of the Confidentiality and Data Protection policy and procedure is available on the intranet and a member of staff will go through this with the customer to make sure it is understood before consent is given.

4.15 Where personal data of a child is processed it shall be lawful where child is at least 16 years old. Where the child is below the age of 16 years, processing will only be lawful if consent is given or authorised by parental/carer responsibility over the child.

5 Processing of Data

Personal data

5.1 Any data relating to a living individual (e.g. name, Date of Birth, sex, address, email address and online identifiers such as IP address, National Insurance Number, education and employment details, address history details of any support services, financial details, photograph(s), bank details, any complaints and supplier details).

5.2 Any information that falls under the definition of personal data, where the data identifies an individual and is not otherwise exempt will remain confidential and will only be disclosed to third parties with appropriate consent.

Sensitive personal data

5.3 Under GDPR sensitive personal data as known as ‘special categories’ (see 4.10) include data relating to medical information, gender, religion, race, sexual orientation, sex life, trade union memberships, political beliefs and criminal record and proceedings, genetics and biometrics.

5.4 In most cases where we share sensitive data we will require customers / employees ‘explicit consent’, unless exceptional circumstances apply or we are required to do this by law. Any such consent will need to clearly identify whom it will be shared with.

Criminal convictions and offences

5.5 Data relating to criminal convictions can be processed if the processing is necessary for performing or exercising our obligations for example under the Employment Law carrying out criminal checks, DBS is necessary.

5.6 Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) (c), where processing is necessary for compliance with our legal obligation, shall be carried out only under the control of official authority, or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

Access rights

5.7 Under GDPR customers and employees have the right of access to their information held by Look Ahead and we must respect and comply with the request. We must ensure individuals can exercise their rights under the legislations.

5.8 The right to prevent the use of the information which is likely to cause damage or distress.

5.9 The right to rectify or destroy inaccurate data, erase and object.

5.10 In the case of 5.4 and 5.7, Look Ahead may refuse the request and still process information in order to fulfil legal obligation as described in section 4 of this policy and procedure.

5.11 Current Customer files will be regularly monitored by line managers to ensure all information is current and up-to-date and if necessary discussed in supervision.

5.12 Checks of customer files may also be monitored through quality assurance. If staff are in doubt about how something should be recorded they should take advice from a more senior member of staff.

5.13 Sensitive information should not be recorded in supervision notes or should be kept separately for manager and employee to review. Some services are checked for quality assurance by the Safeguarding and Quality Team and would require to see staff supervision notes, to comply with the requirements of CQC.

Customers access to personal files

5.14 We are obliged by law to response to information request. We must provide an individual with a copy of the information the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system. See Subject Access Request Policy and Procedure for further information.

5.15 Customers have the right to access their file and it is, therefore, vital that all information recorded is accurate, factual, non judgemental and, where possible, agreed by the customer

5.16 Information request from customers. legal representative and third parties must be sent to the Information Governance Manager to: Myinforequest@lookahead.org.uk

Employees access to personal files

5.17 Each employee has a personal file in the Human Resources Department at Head Office

5.18 Employees can request personal files by giving two weeks written notice to their HR Business Manager at the Head Office.

5.19 The HR Department must keep a log of all requests from staff to view their personal files.

5.20 All Staff requests must be sent to HR@lookahead.org.uk.

5.21 See Appendix 1 for more information of staff access to HR files.

Sharing of customer information

5.22 All customers should complete the Data Protection and Confidentiality form for consenting to sharing their information. See Appendix 2.

5.23 Sharing personal information about customers when it is not necessary for work-related purposes is wholly inappropriate and may result in disciplinary action.

5.24 When discussing personal information about customers, staff should always seek out a private place.

5.25 As a general principle, staff will only have access to files when they need information in order to carry out their duties.

5.26 Information Sharing Agreements must be in place where we are sharing information with third parties and commissioners.

6 Disclosure of Information to Third Party

6.1 It may in some circumstances be necessary to share personal information about our customers with third parties, such as family and friends, benefit agencies or social services.

6.2 Information may only be shared with a third party with the customer's consent. All customers sign a The Data Protection and Confidentially Consent form when they start with Look Ahead setting out who we can share information with.

6.3 If the customer has not given consent to share information with a particular third party, information about that person should only be shared with an appropriate agency for the following reasons:

- Where we have a legal obligation to share the information
- Where there is a duty of care to protect the customer, such as in adult protection cases.
- Where there is a need to inform people for the protection of the public, such as when the customer has committed a crime or specifically threatened a person or persons.

6.4 Requests for customer information from organisations or individuals involved in providing customers with support should only be provided if the third party is authorised to hold information about the customer, if the organisation/individual can assure that the information will be treated in a secure and sensitive manner and if sharing the information would not be a breach of the customer's data protection.

6.5 Information Governance Manager must be informed of any data requests from police, customs or any government agencies.

7 Exemptions from Disclosure of Information

7.1 Under the legislations the exemption from disclosing personal data and sensitive personal data to a customer when they request it, where it is necessary to safeguard a range of interests this includes:

- Where provision of this information would be likely to prejudice the prevention or detection of crime

To protect the rights and freedoms of others (for example where one customer has made a statement about another, or recording behaviour which may indicate drug dealing is taking place).

7.2 Data which is exempt from disclosure should be stored in the confidential section of the customer's file. If a staff member is in doubt about what should go in the confidential section, they should seek advice from their Manager.

8 Storage

Storage of customer files (paper records) within staffed offices

8.1 All customer files must be kept in a secure area and in locked fireproof filing cabinets. Filing cabinets must be located in an area to which the public does not have free access.

8.2 Documents containing confidential or sensitive information should never be left in public view and should be returned to the customer's file promptly.

Electronic records (storage)

8.3 All electronic records containing confidential or sensitive customer information should be stored on a system which is password protected and, where appropriate, access to information should be restricted to users with a genuine need to use it.

8.4 Computer screens should be locked when not attended where confidential data could be accessed.

Electronic records (retention)

8.5 The guidance on retention periods in the procedure covers retention of electronic records of customer information and customers' files, and should be followed in accordance with cross reference to the Archiving Policy and Procedure.

Use of portable equipment

8.6 Confidential personal information which is stored electronically should always be password protected, and data must be held centrally where it can be regularly backed up and stored securely.

8.7 Personal or confidential data should not be stored on the hard drive of a portable computer or net book unless it is supplied by Look Ahead and has data encryption technology installed - please refer to the Network, Email and Intranet policy and procedure for further details.

Use of email

8.8 Confidential or personal customer information should not be sent by email, as emails are sent in clear text which could be intercepted.

8.9 In exceptional situations, where information needs to be sent electronically, customer's personal information should be sent via Egress or encrypted format (see below for further guidance) or personal details removed from all emails to anonymise information. It is also good practice to ensure that the recipient of the email is aware that its contents are of a confidential nature.

8.10 Sending highly confidential customer information via email must be avoided.

8.11 Always check your emails before sending personal data that you have:

- Correct recipient name.
- The right information and not someone else's information.

Email encryption

8.12 To send an encrypted email follow these steps:

- Compose an email message as normal within Outlook 2010
- On the same window you composed your email, click on "options".
- When the "Message Options" window appears, you'll see a drop down menu near the top called "Sensitivity". The default option is "normal", change this to "Confidential", once done select "Close" at the bottom right hand corner of the "Message Options" window.
- This will bring you back to the email you have been composing. Once the email is finished you can send as normal and the message will leave the organisation being encrypted.

Note: This process **ONLY** works for sending emails external to Look Ahead, doing this for an internal recipient **will not** encrypt the email.

Printing

8.13 Always ensure that you check you have selected the right printer, use **locked printing** where possible and collect any confidential information from the printer immediately.

Taking documents outside of staffed services or offices

8.14 It is recognised that staff providing floating support will need to transport documentation containing confidential or sensitive information about customers between appointments.

8.15 Care must be taken to prevent disclosure of confidential information to unauthorised persons by transporting documentation in a secure bag or opaque folder and not leaving it unattended in a public place.

8.16 At no point should files and documents be stored for prolonged periods at home.

8.17 Documents should be returned to the office at the earliest opportunity.

8.18 If it is necessary to take some information from customer files out of the office, the following should be carried out:

- Where possible a photocopy of the form/information should be used as opposed to the original.
- A record should be kept on the customer's file stating which form was copied, the date it was taken, who took it and the date the photocopy was returned to the office and destroyed.
- Confidential information such as the customer's name address should be blocked out.

8.19 When carrying customer documents, a secure holdall should always be used. Documents should **never** be carried in transparent folders.

8.20 Theft of any documents **must** be immediately reported to your Manager and the Information Governance Manager

9 Displaying Information

9.1 Where services wish to display images of customers on display boards, consent must be obtained prior to displaying images. Copy of the consent must be kept on file.

9.2 Customer personal / sensitive personal information **must not** be displayed on notice boards, in public areas (I.e. hallways, communal areas, entrance etc.).

9.3 Where customer and or employees contact details is required for staff use this should only be displayed in a locked office and contain minimal information (I.e. for customers initials and or room number, for employees: first name surname and work contact number / work email address).

10 Archiving, Retention Periods, and the Disposal of Records

Archiving

10.1 The legislations states that "personal data for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes".

10.2 Archived records should be held securely. For more information, see the Archiving Retention and Disposal Policy and Procedure for further information.

Retention periods

10.3 All employees should refer to Look Ahead's Retention, Archiving and Disposal Policy and Procedure to check when archived records should be destroyed, as there are legal obligations to retain certain paper and electronic records for a fixed period of time. The necessary authorisation to destroy records should be obtained from the responsible manager before doing so.

Disposal of paper records

10.4 Confidential information should be disposed of by a specialist contractor or by confidential shredding in specialist disposal bags. Head of facilities should be contacted for arranging the contractor or requesting confidential waste bags.

Disposal of electronic records

10.5 Electronic records containing personal data for former customers should be moved to a secure area of the network where access is restricted to the Manager or Team Leader. Managers should contact IT Team to arrange creation of a secure folder with access restricted to a specific list of staff. The timeframe for review and disposal/deletion of electronic customer records is the same as for paper-based records above.

10.6 Any redundant or unwanted IT equipment which has been used to store data should be reported to the IT Helpdesk. The IT team will arrange secure disposal of IT equipment in line with the IT Disposal policy and procedure to ensure data is disposed of securely.

11 Data and Security Breaches

11.1 Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. Look Ahead has a legal obligation to report any data breaches to the Information Commissioners Office who are the UK supervisory authority within 72 hours.

11.2 Any information that has been lost/stolen emailed to the wrong recipient or becomes available to the general public. The information should be recovered and made secure/properly disposed of as soon as possible. an assessment of the risks associated with this security breach should be made and a Data Breach reporting form must be completed (see Appendix 3), when the information was last seen and what happened. The customer(s) involved should also be informed.

11.3 All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the [name of supervisory authority] of any compliance failures that are material either in their own right or as part of a pattern of failures

11.4 Any member of staff who fails to notify us of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

11.5 All data breaches must be reported to your line mangers and managers must complete the Data Breach reporting form see Appendix 2. Once this is complete please send to the Information Governance Manager at: Myinforequest@lookahead.org.uk

11.6 All security breaches must be brought to the attention of the Head of Information Management and Technology. Again you must complete the Data Breach reporting form.

Evaluate and respond

11.7 An investigation in to the cause of the breach should be completed and appropriate action taken to update security measures and revise procedures accordingly.

11.8 Failure of staff to ensure that the information remains confidential may result in disciplinary action being taken.

11.9 The Information Commissioner can fine organisations up to €20 million or 4% of the annual turnover (which ever is greater) for a "deliberate or negligent" breach of the Data which results in "substantial damage or substantial distress".

12 Closed Circuit Television (CCTV)

12.1 Where Look Ahead is the Landlord It will operate CCTV network for the purpose of crime, prevention and detection and safeguarding.

12.2 See CCTV policy and procedure for more information.

13 Visitors Logs in Services

13.1 Under the legislations and personal data relating to individuals is saved in visitors logs and where the ID of approved visitors is stored on site.

13.2 Visitors log is an everyday part all Look Ahead staffed accommodation based services.

13.3 Visitors logs should contain minimal customer information, initials or room / flat number. Sensitive personal data **must not** be disclosed in visitors log.

Visitors logs and storing copies of ID

13.4 Visitors' logs should only be used if for the safety of staff, customers and the public and for the prevention and prosecution of crime. Any personal data captured in visitor's logs should **only** be used by Look Ahead or any third parties for these pre-determined reasons.

14 Data Handling Training

14.1 All employees must comply with this policy and procedure, if in doubt please contact the Data Protection Manager for further advice / guidance

14.2 Data Handling Training is mandatory and all Look Ahead employees **must** complete the training module, with an 80% pass mark. Line Managers will be responsible for ensuring that employees have completed the training.

14.3 Information Governance Manager will maintain a log and monitor employees that have/have not completed the training.

14.4 Data Handling training will also from part of the induction programme for new starters and a refreshers training.

Appendix 1: Staff Procedure

15 Files and Data held on Employees

Personal records

15.1 Each employee has an electronic record stored on HR System operated by the HR team at Head Office. The data on the system is necessary for the day to day administration of your employment. The data stored includes personal details taken from your application form, your career history with Look Ahead and salary details. Only the HR team have access to the data held on the computer system.

15.2 Should an employee leave Look Ahead, the electronic data will be retained indefinitely in a computerised archive for former employees.

15.3 Each employee also has an electronic personal file. The file is necessary for the overall administration of the employment of staff and to hold the hard copies of the personal details supplied by you, such as your application/curriculum vitae, together with references from previous employers, medical prognosis as to fitness for work, details from appraisals relating to salary progression and any records relating to disciplinary action and any sanction imposed, while that disciplinary sanction is current.

15.4 The files are only seen by staff who have a need to see them, such as your manager and Human Resources staff who process the information. Information is only disclosed when it is relevant and necessary to do so, for example to the Finance department to enable payment of salary. Quality Assurance Team may access your supervision and or training records for quality purpose,

15.5 You may request copies of your electronic file by giving two weeks written notice to your HR Business Partner at Head Office.

15.6 Should an employee leave Look Ahead, the manual personal file will be archived and retained for four years. Only the HR team and / or a Director can retrieve and access archived files.

Training record

15.7 Each employee has an electronic training record stored on Look Ahead's Learning Management System (Academy) operated by the Learning and Development department at Head Office.

15.8 The data on the training system is necessary for the administration of training and personal development programme. The data stored is about the courses staff have attended, courses that were missed/cancelled and courses that are still to be attended. The data is also shared with line managers.

Appraisal and supervision records

15.9 Each employee has a manual appraisal and 1:1 supervision file held by an employee's manager. The file is necessary to keep a record of discussions, targets set and objectives agreed at the annual appraisal interview, six monthly review meeting and supervision meetings. The data on the file is only seen by the manager, except for personal development information which is disclosed to the

Human Resources Department, together with salary increment recommendations which are also disclosed to the Human Resources Department.

15.10 Should an employee transfer or be promoted to another department/project in Look Ahead the file will be transferred to the new manager.

15.11 Employees will be familiar with the content of their file because the notes will have been disclosed before filing. However, in addition you may have access to your file by giving two weeks written notice to your manager.

15.12 Should an employee leave Look Ahead the file should be sent to the Human Resources Department at Head Office and the file will be added to each employee's manual personal file and archived as detailed above.

Recruitment records

15.13 All recruitment records are sent to the HR Department at Head Office immediately after the selection has been made. The HR Department will retain the data of unsuccessful candidates and appointable candidates in secure filing systems for three months and 12 months respectively. Details of successful candidates will form the basis of the individual's personal file.

15.14 While recruitment records are being held by managers, they will be seen only by the recruitment panel and held in a secure filing system.

Payroll records

15.15 Each employee has an electronic payroll record held in the Finance Section at Head Office. The data held on the system is necessary for the administration of employees' pay, including tax and national insurance deductions and pension deductions if applicable. The data stored includes details taken from your application form, your career history and your P45.

15.16 Only the Finance Director and Payroll personnel in Look Ahead have access to these records. Appropriate information is sent to the Pensions Trust, Inland Revenue, Child Support Agencies, Local Authorities and UNISON, where deductions are remitted to these organisations. All payroll details are also submitted to Centre file, our agents who process the monthly payroll and generate payments.

15.17 You may attend Head Office and view your data held on the system by giving two weeks notice to the Payroll Officer in the Finance Department.

15.18 Should an employee leave Look Ahead the electronic data will be retained on the system for one year and then archived on the system and in hard copy form for six years.

Appendix 2: Consent for Sharing Information

DATA PROTECTION AND CONFIDENTIALITY CONSENT FORM

Organisation Name: Look Ahead

Service Name: ……

Service Address: ……

……

Email: ……

Phone: ……

As part of Look Ahead's responsibilities in relation to the Confidentiality and the General Data Protection Regulation, which comes into force in May 2018, I understand that Look Ahead agrees to:

- Only keep information for purposes related to my support or care.
- Make sure that records are accurate and kept up-to-date.
- Make sure that records are kept no longer than necessary. An electronic file and paper file in some service(s) will be kept for maximum of 3 years and 6 years if the service is registered with the Care Quality Commission (CQC).

I understand that the information I share with staff from Look Ahead will be stored securely in a locked filing cabinet / locked office and or on a password protected computer.

I understand that at times it may be necessary to share my information with and from relevant agencies and I therefore give my consent for staff to share this information. I agree that personal information about me may be shared and gathered from the following agencies:

- Hostel
- Landlord
- Leaving Care Service
- Local Authority
- NHS and other Health Services, including my GP practice
- Mental Health Services
- Police
- Prison Service
- Probation Service
- Psychiatrist
- Rehabilitation Services
- Relative / representative (who has authority to act on behalf of customer or is a parent of guardian for young person under 16 years old)
- Social Services
- Safer Neighborhood
- Other: please specify: ……

Exceptions: In this space I have written the names of specific people or agencies with whom I do not want information to be shared.

I understand that apart from necessary information sharing, my personal details will always remain confidential.

The only exception to this will be where Look Ahead has serious concerns about personal safety or are legally required to. Examples of this include:

- If staff believes I am seriously contemplating suicide or self harm.
- Where there is a genuine threat of violence or abuse.
- Where there is a child protection concern.
- Where there is Safeguarding/ DOLs concerns.

What is the personal and sensitive data that Look Ahead will hold about me?

- Personal data about me will include: my full name, date of birth, address, postcode, telephone number, email address and health / diagnosis reports.

- Sensitive personal data about me may include: my racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexuality or sex life, offences or convictions, genetic and biometric data.

I understand it is my right to request access, rectify and or erase my personal data held by Look Ahead.

I understand that I have the right to withdraw consent for Look Ahead to share my personal data at anytime.

I understand that even if I refuse to share my information. Look Ahead may still share my personal data with the agencies in order to fulfil the legal obligation of the tenancy / license agreement and the care and support provided by Look Ahead. This is explained in Look Ahead's privacy notice.

Customers name……..Signature……Date:……

Only complete this section if someone is signing on behalf of the customer.

I am signing on behalf of……

Relationship to customer:……

Your name:……Signature……Date……

Permission to use my photos

From time to time we may use your photos for internal publications, such as Look Ahead's newsletters and other internal publications and we may upload your photos to intranet (The Hub and or Workplace). Your service may also display your photos on notice boards in communal areas, to promote activities and celebrate achievements. We can only do this if we have your permission to use your photos in this way. If you agree, please sign in the box below.

I agree for Look Ahead to use my photos
(Signature for photos is optional)

Appendix 3: Data Breach Reporting Form

The purpose of this document is to ensure that in the event of a data or security breach, the information can be gathered to understand the impact of the incident and what must be done to reduce any risk to the customer /staff whose information has been breached.

The checklist must be completed by manager / service manager with the knowledge of the incident. The completed form must be sent to the Information Governance Officer at: myinforequest@lookahead.org.uk and will be review by the officer who can determine Data Protection Implications and assess whether changes are required to existing business processes.

Summary of the Event	
Date and time of breach.	
Department or service name.	
When was the breach reported?	
How did you become aware of the breach?	
Nature of breach e.g Theft /disclosed in error / loss of data / technical problems / IT security breach.	
Description of how the breach occurred.	
Full description of personal / sensitive data involved (without identifiers).	
Number of people whose data is affected.	
Have all affected individual(s) been informed.	
If not state why not?	
Is there any evidence to date that the personal data involved is this incident has been inappropriately process	

or further disclosed? If so please provide details.	
What immediate remedial action where taken.	
Has the data been retrieved or deleted? If yes please stated date and time.	
Describe the risk of harm to the individual as a result of the breach.	
Describe the risk of identify fraud as a result of the incident.	
For Information Governance Officer	
Do you consider the employee(s) involved has breached information governance's policies and procedures?	
Does disciplinary action need to be taken in relation to the employee(s) involved?	
Has the employee attended Data Protection Training? if not then book them on the course.	
What further action will be taken to minimise the possibility of a repeat such an incident?	
Has this been reported to ICO? If Yes – add the date reported and description of what ICO advised.	

Related documents

Document	Link
Connected Policies	CCTV Policy Subject Access Request Retention Archiving and Disposal Human Resources
Forms and Letters	Data Breach reporting form Data Protection and Confidentiality form
Information Sheet	Yes available on the Hub in Data Protection
Easy Read	
External Websites	http://www.lookahead.org.uk www.housing-ombudsmen.org.uk https://ico.org.uk/for-organisations/guide-to-data-protection/
Legislation/Regulation	• Regulation 19 of the Health and Social Care Act 2008 (Regulated Activities) • Care Quality Commission • Human rights Act 1998 • Data Protection Act (DPA) 1998 and General Data Protection Regulation (GDPR), when this comes into force May 2018. • The Protection of Freedoms Act 2012. • The Police Act 1997. • EU Directive 2017/541 on combatting terrorism. • The Housing Act 1996, s.51 (2) requires that all social landlords have a duty to become a member of any Housing Ombudsman Service scheme approved by the Secretary of State. • Care Act 2014 • Health and Social Care Act 2008 (regulated activities) Regulations 2014 • Mental Capacity Act 2005 • Mental Health Act 1983 • Housing Act 2004 • Homelessness Act 2002 • Homelessness Reduction Act • Children's Act 2004 • Caldicott Principles

Version Control

Version no.		**Date effective:**	May 2018
Brief summary of changes:	New Policy and Procedure		
Colleague consultation:	N/A		
Customers consulted:	N/A		
Results customer consultation:	N/A		
Other consultation:	N/A		
Signed off by:	Claire Luxton		
Author:	Claire Luxton		
Review date:			

King's Building
16 Smith Square
London SW1P 3HQ

Tel: 020 7368 4600
policyresponse@lookahead.org.uk

lookahead.org.uk

Services we would be proud
for our loved ones to receive