HARROGATE NEIGHBOURS HOUSING ASSOCIATION

Title: Data Protection, GDPR & Confidentiality Policy

Policy: HN-HR-27

1. Purpose

1.1. The organisation is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data.

1.2. This policy applies to the personal data of job applicants, employee's workers, contractors, volunteers, Board Members and former employees, referred to as HR-related personal data. Data protection relates to information which is held on file in such a way that individuals may be identified

1.3. The Data Protection Officer is Sue Cawthray and they are to inform and advise the organisation on its data protection obligations. Questions about this policy, or requests for further information, should be directed to the CEO.

2. HNHA Responsibilities

2.1. HNHA will not send unsolicited direct marketing communications to anyone who has indicated that they do not want it and will not pass/share/sell personal data to third parties for their marketing purposes.

2.2. HNHA will seek to ensure all personal data processed is adequate for the specified purpose and limited to only those items relevant.

2.3. HNHA will seek to ensure all personal data processed is accurate initially and updated as necessary.

2.4. HNHA will seek to ensure all personal data is processed is stored and filed consistently and logically, and the data is retained only for relevant periods.

2.5. HNHA will seek to ensure that the level of security is appropriate to the degree of damage or distress that would be caused to the data subject as a result of the loss, theft or damage of personal data.

3. Individuals' Responsibilities

3.1. Helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes his/her bank details.

3.2. Individuals may have access to the personal data of other individuals [and of our customers and clients] in the course of their [employment, contract, volunteer period, internship or apprenticeship]. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to everyone.

4. General Instructions

4.1. The General Data Protection Regulation (GDPR) came into effect on 25 May 2018.

4.2. The Data Protection Bill, which will repeal and replace the Data Protection Act 1998, and as the act obliges HNHA will take 'appropriate technical and organisational measures' to prevent unauthorised or unlawful processing of disclosure of personal data. The measures we will take to protect the loss of personal information will include:

- Technical
- Need to know access only to paper and electronic files
- Password Protection
- Encryption

5. Making a subject Request

5.1. As a data subject, individuals have a number of rights in relation to their personal data. Individuals have the right to make a subject access request.

5.2. If an individual makes a subject access request, the organisation will tell him/her:

- Whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers, for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights;
- and whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

5.3. The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

5.4. If the individual wants additional copies, the organisation will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

5.5. To make a subject access request, the individual should send the request to info@hnha.co.uk or use the organisation's form for making a subject access request. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify his/her identity and the documents it requires.

5.6. The organisation will normally respond to a request within a period of one month from the date it is received.

5.7. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell him/her if this is the case.

5.8. If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify him/her that this is the case and whether or not it will respond to it.

6. Data breaches

6.1. If the organisation discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.

6.2. If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

7. Definitions

7.1. Personal data is any information that relates to a living individual who can be identified from that information.

7.2. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

7.3. Special categories of personal data means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

7.4.
offences, and information relating to criminal allegations and proceedings.

8. Data security

8.1. The organisation takes the security of HR-related personal data seriously.

8.2. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

8.3. Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data

Subsection: CCTV

1. Purpose

1.1. The purpose of this policy is to ensure:

- That the use of CCTV adheres to the principles of the Data Protection Act 1988, the Human Rights act 1998, the Regulation of Investigatory Powers Act 2000 and other relevant legislation.
- That any CCTV system is not abused or misused.
- That CCTV is correctly and efficiently installed and operated.
- That all personnel can be assured of the safeguards in place

2. Introduction

2.1. HNHA places the health, safety and welfare of its staff, contractors and visitors amongst its priorities and aims to ensure it maintains safe and secure conditions throughout the organisation. To assist with these responsibilities, The Cuttings are using the closed-circuit television technology to monitor the outside of the premises and the corridors past the progressive door only.

2.2. This policy sets out the appropriate actions and procedures which must be followed to comply with the Data Protection Act in respect of the use of closed-circuit television (CCTV) services within The Cuttings. Should members of staff have any difficulties with understanding any aspect of this policy, or require further information in respect of accessibility, interpretation or application of the policy, they should contact their Line Manager.

2.3. The use of CCTV is to control the perimeter of The Cuttings and main corridors past the progressive door for security purposes and has been deemed to be justified by the Trustees and Senior Management Team

3. Scope

3.1. This policy applies where HNHA has deployed CCTV within premises occupied by HNHA employees/tenants/visitors/ volunteers & contractors working in buildings that has CCTV installed.

4. Responsibilities

4.1. In order to fulfil its responsibilities in accordance with legislation, the responsibilities for CCTV within HNHA will be as follows:

4.2. Chief Executive /Senior Information Reporting Officer (SIRO)

- The Chief Executive has corporate responsibility for the approval of any CCTV equipment, monitoring the effectiveness, ensuring the Independent Commission Officer CCTV Code of Practice is available through the HNHA Drive and that clearly defined procedures are in place on how to use the system.

- The Chief Executive delegates the responsibility for installation and maintenance of CCTV equipment to the Scheme Coordinator at The Cuttings and the COO at Heath Lodge.

4.3. The CEO is responsible for:

- Ensuring that the organisation complies with the HNHA CCTV policy and guidelines.
- Ensuring that members of staff who have the responsibility for the operation of HNHA CCTV technology are appropriately trained in its use.
- Ensuring the CCTV images are only accessed by those authorised to have access to the stored images through the implementation of adequate authorisation procedures on or off site of the CCTV.
- Ensure that camera control is not infringing on individual's reasonable expectation for privacy in public areas.

4.4. The Scheme Manager and the designated person in her absence have day to day responsibility for ensuring the CCTV cameras are working and is required to report any issues to the appropriate responsible person (see below)

4.5. Line Managers: are responsible for ensuring that staff and volunteers working within their locality/site where CCTV is in operation are aware of this policy and implements its requirements. We currently have CCTV systems located on our main corridors past the progressive door and at various points outside the man building.

5. Use of CCTV

5.1. HNHA CCTV will only be used for the following purposes:

- Crime prevention, detection and security
- Apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings)
- Interest of public and employee health and safety
- Protection of HNHA property and assets
- Assist in lone working safety

5.2. Cameras and other associated recording technologies must not be used to record conversations between individuals as this is highly intrusive and is unlikely ever to be justified. If technologies are installed that have voice recording facility this must be switched off or disabled at all times.

5.3. Any staff misuse of CCTV will lead to disciplinary proceedings.

6. Installation

6.1. Prior to installation, HNHA must ensure that the requirement for CCTV is legitimate and justified:

- All cameras will be located in prominent positions and be used only to monitor the intended spaces.

- They will not infringe on surrounding properties or on personal workspace including individual offices, toilet areas.
- Where cameras unavoidably do cover certain work areas such as corridors, staff working in these areas should be made aware of where the cameras are located and the reasons for having the cameras.

6.2. The location of the camera equipment and the way in which the images are captured must comply with the requirements of the Data Protection Act and the ICO CCTV Code of Practice. This includes ensuring that media used to record images are data compliant and that the images are of suitable quality to ensure that they are fit for purpose.

6.3. All cameras and CCTV systems installations must be installed by competent person. During the approval process a Risk Assessment should be carried out. The Risk Assessment should be used as a basis for the assessment which will be carried out by the responsible person in liaison with their relevant Senior manager.

7. Maintenance

7.1. All CCTV equipment must be regularly serviced and maintained as part of a scheduled programme of maintenance. Testing must ensure that only the designated areas are monitored, and high-quality pictures are available in live and play back modes and in printed format.

8. Signage

8.1. Where HNHA has the responsibility for CCTV installations and operations, appropriate information signs will be erected in all areas of HNHA premises and throughout the site where CCTV coverage is in operation to ensure staff and visitors to HNHA premises are aware they are entering an area that is covered by CCTV surveillance equipment.

8.2. The Code of Practice requires that signs must be placed so that the public are aware that they are entering a zone which is covered by CCTV. The signs must contain of the name of the person responsible for the operation of the scheme, the purpose of the scheme and the details of the person to contact regarding its operation.

9. Information Governance

9.1. HNHA will comply with all of the requirements of the ICO Code of Practice.

10. Use of CCTV footage for disciplinary purposes

10.1. In the event that recorded CCTV footage reveals activity that HNHA could not reasonably be expected to ignore than the relevant CCTV footage may be considered during the investigatory stages of the process and later used in a formal disciplinary hearing if relevant to the allegations against the employee.

10.2. Activity that HNHA could not reasonably be expected to ignore includes acts which constitute gross misconduct in accordance with HNHA's disciplinary policy, as set out in relevant section of staff handbook and/or practices which seriously jeopardise the health and safety of others.

10.3. If such CCTV footage is identified the information will be presented to the employee wherever possible.

10.4. The employee will not be required to make a data subject access request and will have the opportunity to explain or challenges the CCTV content.

10.5. If HNHA identifies that CCTV is relevant to formal proceedings than the timescale for retention of images may be extended for a period of up to 2 years to allow for the completion of the disciplinary procedures including any appeals process and statutory reporting to professional bodies.

11. Data Recording, Storage, Retention and Disposal

11.1. CCTV images must only be used for the intended purposes. Documentation and records relating to the CCTV system will be confidentially retained in accordance with the arrangements, responsibilities and timescales in the HNHA's document Storage, Retention and Disposal Policy.

11.2. The method to secure recorded images will be auditable and audited regularly. This will include, logging of those people allowed access, the method of access and control of images taken from the system and the tracking any hard disk drives that have been removed from the site. All images will be digitally recorded and stored securely within the systems hard drives. Automatic erasure/overwriting takes place after 30 calendar days or sooner.

12. Subject Access

12.1. Under the Data Protection Act, employees and members of the public are entitled to access their recorded images and to a copy of their data in intelligible format. Requests must be made in writing as per the subject access request policy.

12.2. When accessing images two authorised senior staff must be present and a written record made of access will be made. Records of access will be kept.

13. Review of Procedures

13.1. The use and continued requirement of CCTV will be reviewed on an annual basis by the Scheme Manager.

14. Breach of Policy

14.1. A breach of this policy may be regarded as an offence and the member(s) of staff involved may be subject to investigation in accordance with HNHA Information Governance Policy.

15. Discovery of Covert Surveillance Equipment

15.1. Any member of staff who discovers surveillance equipment installed by people who use the service, or their relatives should inform their line manager immediately. Out of hours this should be reported to the on-call senior manager.

15.2. Deliberately damaging the surveillance device, deleting recordings or removing the device with the intention of not returning it to its legal owners is likely to be a criminal offence. However, switching a camera off, or removing it for safekeeping and return to its owner would not be. (CQC Guidance Using Surveillance).

16. Complaints Procedure

16.1. Should members of staff or volunteers have any concerns regarding the operation of HNHA CCTV system these should be raised with their line manager in the first instance.

16.2. If necessary, they may be progressed though HNHA Grievance Policy.

16.3. Members of the public with LLH CCTV concerns should raise this through the HNHA policy and procedure for the management of complaints, concerns, comments and compliments.

17. Policy Review

17.1. This policy will be reviewed every four years' in line with HNHA review process from its effective date to ensure that arrangements put in place are appropriate to operating requirements of HNHA.

CCTV AUDIT/CHECKLIST

A guide to the Privacy Act for Organisations'

Audits of the system must be carried out at least annually and the results reported to the CEO and the SMT. Summary of guidelines and checklist.

1 Deciding whether CCTV is right for you

Clearly identify what you need CCTV for. This is your purpose for using CCTV. Carefully consider whether CCTV will actually meet your needs. Identify:

- the existing problem you seek to address;
- whether CCTV could address that problem and, if so, how; and
- whether there are other alternative options available.

Think about whether it would be useful to consult with people who will be affected. If so, talk to them. You should repeat the steps above when expanding existing CCTV systems, and at regular intervals during the life of a CCTV system.

2 Have a clear plan

Develop a business plan for the CCTV system, setting out:

- the purpose of the system;

- the outcome/s that you expect;
- the type of technology and equipment that will be used;
- how the system will be operated; and
- how privacy impacts will be minimised.

Where appropriate, consult with the community and other key stakeholders on your business plan. Appoint a person to be responsible for the operation of the CCTV system. Develop a clear policy on how images collected by CCTV will be handled. Make this policy easily accessible (for example, on your website). Train staff in your policies and procedures for the CCTV system.

3 Selecting and positioning cameras

Choose equipment which will achieve the purpose of your system in the most privacy friendly way. Where feasible, also use 'privacy enhancing technologies'. Position cameras in a way that will not intrude to an unreasonable extent on the privacy of individuals.

4 Make people aware of the CCTV

Erect signs both near the CCTV cameras and at the perimeter of the CCTV system's range (before individuals enter the range of the cameras) to notify people that cameras are operating. The signs should make clear who owns and operates the CCTV system and the contact details of that agency (if this information is not already obvious). Make sure there is a full privacy notice on your website, or in hard copy at your reception desk, to let the public know more about the operation of the CCTV cameras. If you are installing a system with a major public impact (such as a local council scheme), put notices in the media. Ensure your staff can answer questions from the public about the system

5 Collecting only necessary images

Limit the hours that the CCTV cameras operate to times where it is necessary (such as opening hours, or days and times during the week when crime peaks).

6 Using the CCTV images

Take reasonable steps to check CCTV images are accurate, complete, relevant and not misleading before you use them. Only use or disclose the images you collect with CCTV cameras for the original purpose you collected them. Do not publicly disclose images collected using CCTV unless you have the consent of the individual(s) shown in the footage or you have consulted the Police. Follow the policy you developed under guidelines

7 Storage and retention of images

Ensure that CCTV images are protected from loss and unauthorised access, use, modification and disclosure. Only keep CCTV images for a specified time. This time period must not be longer than is necessary to achieve your purpose.

8 Controlling who can see the images

Ensure that the control or monitoring room is only accessible by authorised staff members. Establish procedures for individuals to access images of themselves captured by your CCTV cameras. Establish procedures for when and how you disclose your CCTV images to the Police. Keep a log of all accesses to CCTV images by external parties.

9 Audit and evaluation

Collect statistics about your CCTV system to allow you to assess its strengths and weaknesses. After a year of operation and at regular intervals afterwards, evaluate the operation of the system to determine its effectiveness and continuing viability. Do regular audits of your equipment and procedures to ensure the system is operating smoothly. Check that your staff or CCTV operators are complying with your policies.

Subsection: Computer Security and Operation Policy

1. **Purpose**

1.1. The company regards the integrity of its computer system as central to the success of the organisation. Its policy is to take any measures it considers necessary to ensure that all aspects of the system are fully protected.

2. HNHA Responsibilities

2.1. Overall computer security is the responsibility of the CEO. Line managers are responsible for security within their own departments.

2.2. Job applicants will be questioned on their computer experience. The implications of their software knowledge will be discussed as appropriate before a job offer is made. All references will be checked. On induction employees will be required to read the key companies' policies as agreed with you line manager.

2.3. The credentials of all temporary, freelance and consultancy staff will be checked in as much detail as possible before they are allowed access to the computer system.

2.4. Computer training at every level will emphasise the importance of security.

2.5. Line Managers and senior staff are responsible for ensuring that basic procedures are followed. Procedures may be bypassed only with the combined consent of the line manager, and a written record must be kept.

2.6. Employees are permitted access only to those parts of the computer system which they need to enter in order to carry out their normal duties. Levels of access will be decided by the CEO.

2.7. Employees may access the internet but access to certain sites will be blocked.

2.8. All incoming emails will be monitored and scanned for viruses before being released to the recipient. Employees with access to personal data are in a particularly sensitive position and must bear in mind at all times the provisions of the Data Protection Act.

2.9. Passwords must be used at all times and changed regularly and shared with the EA. Employees should not select obvious passwords. All passwords must be kept confidential. Employees must not give their passwords to other members of staff or to

any person outside the organisation. Password protected sites should be closed when finished with and computers switched off. Computers should not be left open and unattended.

2.10. When an employee with access to personal data leaves the organisation all passwords in that department will be changed.

2.11. Regular checks will be made for viruses by the IT department.

2.12. No external software may be used without authorisation by the CEO.

2.13. No private work or computer game playing is permitted.

2.14. Misuse of computers is a serious disciplinary offence. The following are examples of misuse:

- fraud and theft
- system sabotage
- introduction of viruses, etc
- using unauthorised software
- obtaining unauthorised access
- using the system for private work or game playing
- breaches of the Data Protection Act
- sending abusive, rude, or defamatory messages or statements about people or organisations, or posting such messages or statements on any websites or via email
- attempting to access prohibited sites on the internet.
- hacking
- breach of the organisation's security procedures.

2.15. All staff that use a PC must complete Cyber Essentials Training and complete a short quiz afterwards, the quiz is then filed in their HR file, cyber risk to be added to the training matrix and should be completed every 2 years. The line manager is responsible to ensure this happens.

2.16. This list is not exhaustive. Depending on the circumstances of each case, misuse of the computer system may be considered gross misconduct. Please refer to the disciplinary rules and procedures. Misuse amounting to criminal conduct may be reported to the police.

2.17. Management, in consultation with specialist auditors, may institute confidential control techniques and safeguards. Financial systems are subject to special reconciliation processes.

2.18. Senior managers will meet regularly to review computer security.

2.19. All breaches of computer security must be referred to the relevant director or to the general manager. Where a criminal offence may have been committed the board will decide whether to involve the police.

2.20. Any member of staff who suspects that a fellow employee is abusing the computer system may speak in confidence to the general manager.

3. Display Screen Users

3.1. We recognise the responsibility to ensure that all staff using display screens are encouraged to visit their optician annually for the opportunity to be screened.

4. General Instructions

4.1. Display screen users are defined as follows: -

- A member of staff who depends on the use of a visual display unit (VDU) to perform his / her duties.
- A member of staff who uses VDU equipment more or less daily.
- A member of staff who uses a VDU for continuous periods of an hour or more at any one time.

4.2. Any member of staff who complies with the criteria above has the right to an eye and eyesight test annually.

4.3. The test will be performed by the individual staffs Optician.

4.4. In the event of an employee having visual problems as a result of using VDU equipment, HNHA will provide a single lens special corrective glasses with standard frames, specifically for the Display Screen Equipment Regulations. The staff concerned must discuss this with the Chief Executive to ascertain whether any reported problems may be referred to the Occupational Health Department at the Trust via their Optician or General Practitioner.

4.5. If an employee has visual problems between the annual tests, further tests may be arranged.

5. Computer and Printer Problems

5.1. HNHA recognises the advantages of information technology with access by the management team.

5.2. Management also recognises the importance that all staff who have computer access, must familiarise themselves with action to be taken in the event of computer breakdown.

6. General Instructions

6.1. In the event of computer breakdown, either hardware or software, the member of staff discovering the problem should:

- Perform a shutdown and start up by clicking the ‘Start’ button and selecting ‘shutdown’. Once the computer has completely shut down, turn it off at the mains, wait 3 minutes and then switch it back on.
- If the problem persists then contact the Executive Assistant in the first instance and explain the problem.
- The Executive Assistant will log the problem with Razor Blue through servicedesk@razorblue.com or telephone support on 0333 344 6344.

- RazorBlue will contact you directly to talk you through step by step.
- For a password re set you can contact RazorBlue directly.

6.2. Any printing problems must be reported to Admin office who will then report it to IT Clarity Office Solutions 01423 795426

Subsection: Confidentiality

1. Purpose

1.1. To protect clients, staff, volunteers and trustees.

2. HNHA Responsibilities

2.1. HNHA views confidentiality very seriously and therefore ensures that all healthcare professionals, volunteers, trustees and employees respect the confidentiality of all its clients, volunteers and staff.

3. General Instructions

3.1. Staff must respect confidential information obtained in the course of professional practice and refrain from disclosing such information without the consent of the clients, staff or person entitled to act on his/her behalf. Except where disclosure is required by law or by order of a court, or is necessary in the public interest.

3.2. All staff/volunteers should not on any account disclose information acquired about the affairs of HNHA or its associated companies to any unauthorised member of staff/volunteer/client or to anyone outside the employment of HNHA.

3.3. Staff working from home to ensure the Policy HN-HR-7 Working from home policy is read.

3.4. Staff, volunteers and trustees should not remove any document or written information pertaining to the business of HNHA, or copies thereof, or any other articles, which are the property of HNHA, without the express permission of the CEO. All staff should treat information and personal details, both verbal and written about each other in complete confidence and respect.

3.5. Family and Friends - Staff should never risk assess or provide services for a service user who is known to them in any other than a professional capacity. Staff should alert their line manager if this situation should occur so that alternative arrangements can be made which will not jeopardise the needs of the service user.

4. Procedure

4.1. Transferring of any confidential information to other organisations including other services involved in care and support must ensure the following:

- A standard letter (copmust be sent and a reply received establishing the receiving organisation complying with the Data Protection Act 2018 and has the systems to maintain confidentiality.

- The expressed permission of the service user is given (or Next of Kin or advocate).
- Any non-compliance must be referred to the CEO.

4.2. Deliberate breaches of confidentiality other than with the consent of the individual should be exceptional and may be viewed as a serious disciplinary offence.

4.3. Taking photographs, and videos of clients by visitors is not allowed. Photos and videos taken by the staff for social media and the TV Screen must have written consent from the client and or their relative/friend and recorded by the managers.

4.4. This policy is a mandatory requirement to be read and signed for at the Induction stage. Volunteers must also read and understand.

4.5. Access to the computer system is controlled by the CEO, and is password protected, and will be spot-checked from time to time by the CEO. IT information must be treated in the same manner as written or verbal information. Any misuse of information accessed on the computer is subject to disciplinary action as it is an act of gross misconduct.

4.6. Staff who wish to access their emails on a mobile device must only do so on their issued HNHA mobile. No employees are permitted to access their emails on their personal device. Emails must only be accessed using the Microsoft Outlook Application and Multi Factor Authentication must be added.

4.7. With the exception of data which is public knowledge, no data pertaining to HNHA or it's stakeholders should be accessed using an employee's personal device.

_____

Signature of Chief Executive

Review as HNHA KPI

Due November 2025