Name of policy	**Data Protection & Access Policy**
Policy Owner	Resources Director
Agreed date of implementation	September 2019
Date of review	September 2021

"Protecting personal data"

1.0 Purpose

1.1 Nottingham Community Housing Association (NCHA) processes data. This must be done in a compliant fashion. Current legislation is the Data Protection Act 2018 & the GDPR 2016. Data is a valuable asset of NCHA & it must be treated appropriately

2.0 Scope

2.1 This policy relates to personal data as defined by the GDPR 2016 and NCHA's data collection purposes as set out in its registration with the Information Commissioner's Office. It applies to any processing of NCHA's data. It applies to all records regardless of format.

2.2 This policy will from part of NCHA's information governance framework and should be used in conjunction with that framework.

3.0 Glossary

3.1 Terms are defined in law (data protection act 2018 & GDPR). The layered guide gives clarification for NCHA

4.0 Risks

4.1 Failure to comply with the DPA could lead to significant legal, financial and reputational adverse impact for both the Organisation and for individuals

5.0 References

- ICT Security Policy
- Housing Management Manual
- Document retention schedule
- Departmental DPA procedures
- CS Quality Manual
- Data Protection Act
- General Data Protection Regulation
- Financial Regulations
- ICO website
- Breach reporting procedure

6.0 Data Protection Compliance at NCHA

6.1 NCHA as Data Controller takes responsibility for the processing of Personal Data and ensuring that data is processed in accordance with the Legal principles and with NCHA's CLEAR values.

6.2 NCHA is registered with the ICO for the collection and processing of personal data under six defined purposes and our internal ICO contact is the **Cyber security and Data protection manager (DPO).**

7.0 Data Collection and Data Subjects

7.1 NCHA's data subjects are the individuals we process Personally Identifiable Information for. This includes, but is not limited to all of NCHA's stakeholders, contractors and business contacts.

7.2 Data subjects have a number of rights granted under the law. It is important that these rights are recognised & respected.

7.3 Data subjects are responsible for the data they provide NCHA. They must ensure it is accurate & up to date.

7.4 All Questions and enquires must be directed to the Data Protection Officer. This enables us to provide a consistent approach to data protection across the organisation.

8.0 Data storage and processing

8.1 Data stored or processed by NCHA using NCHA's systems or accessed via NCHA systems must conform to the ICT security & access policy. This includes cloud based services.

8.2 Departmental managers are responsible for effective information management and implementation of this policy. This can be done via the GDPR champions group and direct liaison with the DPO. Departmental managers are responsible for updating the required documentation and notifying any changes to their processing activities.

8.3 **Working out of the office**
Managers should be aware of any data that colleagues use to work out of the office, this includes site visits, working from home and away days. This data must be kept secure and limited to only the data necessary.

8.4 **Security**
Measures need to be taken to prevent accidental or unauthorised removal, access, loss, destruction, damage or processing of data. These measures are outlined in the ICT security policy and the Personal information protection and access policy.

Bear in mind the points below:

- Take steps to control physical security (keeping sensitive data in locked filing cabinets, complying with the clean desk policy etc.)
- Putting information access controls in place and using them (e.g. not sharing your username and password)
- Notifying mangers if you suspect a breach has taken place – see point 8.6

8.5 **Destruction**
Paper records containing sensitive/personal data (such as tenant/service users contact details) need to be securely destroyed, it is recommended that any paperwork containing this data is shredded. Paperwork containing medical details, diary notes and other very sensitive information must be destroyed using the secure shredding service.

8.6 **Lost/Stolen/Misused Data**

Suspected loss, theft, unapproved access, or misuse of any data must **immediately** be reported to your line manager who must then inform the Technology department (preferably The DPO).

If possible please include the following information.

1) What data has gone missing
2) When did the data go missing
3) What format was the data in (paper/electronic)
4) What device was the electronic data held on (e.g. Laptop, smart phone)
5) Have the police/insurers been informed

NCHA now have a duty to report breaches to the ICO within 72 hours.

9.0 Data Access

9.1 All personal information held by NCHA is confidential and can only be accessed for a specific purpose and with the relevant authority. All Data sharing agreements must be agreed and stored centrally.

9.2 Personal data will not be used for direct marketing.

9.4 **Subject Access Requests**

The subject on whom the Association holds a record is entitled to have access to the personal data within Thirty days of the request being made, provided that:

- They can provide appropriate evidence as to their identity;
- Information emanating from, or concerning other people has been removed from his/her record;

9.5 All requests for access to personal data must be made in the first instance to: ***The Cyber security and Data protection manager (DPO)***.