Data Protection Policy

1. Introduction

1.1 We are committed to compliance with the Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (UK GDPR).

2. Purpose

2.1 We must process personal data to carry out our every day business, deliver service and fulfil our corporate functions and objectives.

2.2 We must comply with the DPA and UK GDPR when processing personal data. Non-compliance may lead to damage or distress for our customers, tenants and / or workers, claims for compensation, reputational damage, and / or regulatory action from the Information Commissioner's Office (ICO) such as a fine of up to €20 million or 4% of global turnover.

2.3 The DPA and UK GDPR, and Article 8 of the Human Rights Act 1998, indicate that our processing of personal data should strike a balance between our need to function effectively and efficiently, and our respect for the rights and freedoms of data subjects.

2.4 This Policy sets out how wewill comply with our statutory requirements and safeguard the rights and freedoms of data subjects.

3. Scope

3.1 This Policy applies to all workers and data processors; this includes full and part time employees, agency or temporary workers (including volunteers) or contractors, and individuals on work experience placements.

3.2 This Policy applies to information assets that we are responsible for, specifically manual and electronic personal data records.

4. Policy

4.1 Definitions

4.1.1 Personal Data are any information that can directly or indirectly identify a data subject. This includes a wide range of 'identifiers', such as names, identification numbers and location data.

4.1.2 Special Categories of personal data are any information about a data subject's biometrics, ethnic or racial origin, genetics, health, political opinions, religion, sex life, sexual orientation and trade union membership.

4.1.3 A Data Controller will decide why and how personal data are processed. Data controllers will usually be organisations such as ours, but could be individuals in limited instances such as self-employed consultants. An employee cannot constitute a data controller.

4.1.4 A Data Processor will process personal data on behalf of the data controller. An employee cannot constitute a data processor.

4.1.5 A Data Subject is a living person to whom the personal data relates.

4.1.6 Processing is any operation performed on personal data, whether or not by automated means, for example collection, disclosure, recording, retrieval, storage, transmission and use.

4.2 Roles and responsibilities

4.2.1 All workers have a duty to help us to process personal data appropriately and effectively. Specific categories of workers have duties as per Clauses 5.2-5.4.

4.2.2 Leadership Team, Senior Information Risk Owner (SIRO) and Deputy SIRO:
- Oversight and support of corporate data protection compliance.

4.2.3 Information Governance Team (IGT), which includes the Data Protection Officer:
- Advice on data protection;
- Provision of data protection training;
- Drafting and review of data protection policies;
- Handling of requests from data subjects, such as subject access requests;
- Advice on information security;
- Managing personal data breaches; and
- Updating our entry on the ICO Public register of data controllers.

4.2.4 Workers:
- Completion of mandatory data protection and information security training;
- Compliance with data protection and information security policies;
- Keeping personal data secure;
- Reporting personal data breaches and requests from data subjects (for example, subject access requests) to the IGT.

4.3 Data protection training

4.3.1 We recognises that data protection training is crucial for all workers to understand their roles in respect of our compliance with the DPA and UK GDPR.

4.3.2 Workers must complete the mandatory data protection and information security training on an annual basis. This includes the relevant e-learning for network users, hard copy alternatives for non-network users and bespoke training where this need is identified. All managers are responsible for ensuring that workers complete the training in practice.

4.3.3 Workers with advanced data protection responsibilities must complete additional training where this is made available and they are instructed to do so.

4.4 Data protection training

4.1.1 We recognises that data protection training is crucial for all workers to understand their roles in respect of our compliance with the DPA and UK GDPR.

4.4.2 Workers must complete the mandatory data protection and information security training on an annual basis. This includes the relevant e-learning for network users, hard copy alternatives for non-network users and bespoke training where this need is identified. All managers are responsible for ensuring that workers complete the training in practice.

4.4.3 Workers with advanced data protection responsibilities must complete additional training where this is made available and they are instructed to do so.

4.5 Personal data processed

4.5.1 A detailed description of the types of personal data that we process and the purposes for that processing are included in our entry on the ICO Public register of data controllers under the registration number ZA304342. The IGT will ensure that our entry is kept up to date.

4.6 Data protection principles

4.6.1 We will comply with the six data protection principles by implementing robust processes to ensure that personal data are:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and not limited to what is necessary;
- accurate, and where necessary, kept up to date;
- kept in a form which permits the identification of data subjects for no longer than is necessary; and
- processed in a manner that ensures appropriate security, using appropriate technical or organisational measures.

4.6.2 We will also process personal data in accordance with our Information Security Management System (ISMS) and other related policies and procedures, in particular to ensure the security of personal data.

4.7 Privacy notices and CCTV

4.7.1 We will ensure that we maintain appropriate privacy notices to inform data subjects about how we will process their personal data.

4.7.2 We will adhere to the ICO CCTV code of practice in respect of our CCTV. Whilst not mandated by the Protection of Freedoms Act 2012, We will also recognise the standards set down in the surveillance camera code of practice to operate legitimate surveillance. Where appropriate, We will be transparent in our use of CCTV and similar surveillance equipment, and monitoring spaces to which the public, residents, service users and workers have access; we will also ask partner organisations involved in joint or multi-agency initiatives to mirror this approach.

4.8 Personal data breaches

4.8.1 Workers must report all actual or suspected personal data breaches or near misses immediately or as soon as reasonably practicable within 24 hours of discovery to the IGT via IG@boltonathome.org.uk. The reporting, assessment,

response and notification of breaches or near misses will be in accordance with statutory requirements and other related policies and procedures.

4.9 Data subjects' rights

4.9.1 Data subjects have the following rights, subject to exemptions, under the DPA and UK GDPR:

- to be informed about our collection and use of their personal data;
- to withdraw their consent at any time, if we are relying on their consent as a basis and / or condition for processing;
- to make a subject access request for a copy of their personal data;
- to request that we correct their personal data if it is inaccurate or out of date;
- to request that we erase their personal data where it is no longer necessary for us to retain it;
- to request a restriction is placed on further processing where there is a dispute in relation to the accuracy or processing of their personal data;
- to request that we provide them with their personal data and where possible, transmit that data directly to another data controller;
- to object to the processing of their personal data; and
- to not be subject to automated decision making including profiling.

Workers will promptly forward such requests to the IGT immediately or as soon as reasonably practicable within 24 hours via IG@boltonathome.org.uk. Our handling of such requests will be accordance with statutory requirements, other related policies and procedures, and relevant ICO guidance such as the ICO Right of access guidance.

4.9.2 We will ensure that we respond to all subject access requests within one month. Where requests are complex or numerous this may be extended for a further two months. We will ensure the requestor is informed about the extension within one month of receipt. All subject access requests must:

- be made in writing (paper or email) preferably to IG@boltonathome.org.uk and accompanied by adequate proof of identity and where applicable, written authorisation. Additional guidance outlining suitable types of identity and authorisation plus an optional Subject Access Form is made available on our website;
- specify clearly and simply the information required;
- give adequate information to enable the requested data to be located;
- be accompanied by the relevant fee where appropriate; and
- make it clear where the response should be sent.

Whilst the DPA and UK GDPR do not limit the number of subject access requests an individual can make to any organisation, we will not be obliged to comply with an identical or similar request to one already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones. On this basis we reserve the right to refuse unreasonable repeat requests received from the same person for the same or similar information within 12 months of a previous request.

4.9.3 Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we may:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

4.9.4 If a data subject remains dissatisfied with how we have responded to their request under Clause 11.1, they may ask for the matter to be dealt with under the appropriate complaints procedure, or in the case of a worker, under our grievance procedures.

4.9.5 If a data subject continues to be dissatisfied at the conclusion of our complaints or grievance procedures, they may write to the ICO via Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or casework@ico.org.uk, to request an independent assessment.

4.12 Data protection impact assessments (DPIAs)

4.12.1 We will ensure that any new or altered processing identifies and assesses the impact on a subject's privacy as a result of any processing of their personal data, via a DPIA. Our DPIAs will be in accordance with statutory requirements, other related policies and procedures and relevant ICO guidance such as the ICO DPIA Guidance.

4.13 Data processors

4.13.1 Where we instruct data processors, such as external agencies or companies to undertake the processing of personal data on our behalf, this must be covered by a written contract which complies with DPA and UK GDPR requirements including clauses that the data processor only act on our instructions, take appropriate measures to ensure the security of processing, promptly notify us of personal data breaches and the exercise of data subjects' rights, and permit us to audit their processing. Our relationship with data processors will be accordance with statutory requirements, other related policies and procedures, and relevant ICO guidance.

4.14 Data sharing

4.14.1 Where we enter into ongoing and routine data sharing with one or more other data controllers, this must be covered by a Data Sharing Agreement which includes a statement of compliance signed by the participating organisations, specifies the relevant basis and conditions for processing, the personal data to be shared, and outlines provisions in respect of accuracy, consent, fair processing, retention and security. Our data sharing arrangements will be accordance with statutory requirements, other related policies and procedures, and relevant ICO guidance such as the ICO Data sharing code of practice.

4.15 Disclosures

4.15.1 We may be required to make one-off disclosures of personal data, for example to comply with a court order, or other legal requirements including prevention or detection of crime, apprehension of an offender or gathering of taxation. Workers will promptly forward such requests immediately or as soon as reasonably practicable within 24 hours to the IGT via IG@boltonathome.org.uk to facilitate handling in compliance with statutory requirements. Our handling of disclosures will be accordance with statutory requirements, other related policies and procedures, and relevant ICO guidance.

4.16 Data matching

4.16.1 We will only use data matching techniques for specific lawful purposes and will comply with any relevant ICO guidance.

4.17 Monitoring of workers

4.17.1 We reserves the right to vet and verify our actual and prospective workers, and to monitor telephone calls, email and internet access in compliance with relevant legislation. We will handle this in line with relevant guidance issued by the ICO, such as the ICO Employment Practices Code.

4.18 Further guidance

4.18.1 We will support this Policy by associated training, awareness raising and additional guidance on the intranet.

4.18.2 The ICO website contains a large range of data protection resources and guidance for use by organisations and the public, such as the Guide to UK GDPR.

5. Equality and Diversity

An analysis was carried out and determined no impact on individuals.

6. Consultation

6.1 The IGT did not conduct external consultation in respect of the formation of this Policy.

7. Legal / regulatory requirements

7.1 This policy ensure compliance with the Data Protection Act 2018 and UK General Data Protection Regulation

8. Related policy and strategies

8.1 List any polices that will be considered alongside your policy.

9. Responsibility, monitoring, review and evaluation

9.1 We will monitor and review our processing activities to ensure these are consistent with the principles of data protection legislation and to facilitate continual improvement.

9.2 Serious breaches of this Policy caused by deliberate, negligent or reckless behaviour may result in disciplinary action in line with our HR policies.

Date approved	Arcon Board 4 February 2020 Group Board 12 February 2020