Abbeyfield Lytham St Annes
1 Park Avenue
Lytham St Annes, FY8 5QU

DATA CONFIDENTIALITY, PRIVACY, PROTECTION & RETENTION POLICY

1. Context, aims & objectives of this policy

Our Society holds the data we need for regulatory and management purposes. We recognise our obligations regarding confidentiality and our legal obligation to safeguard the data we hold and will respect and protect the privacy of our residents, staff, trustees, volunteers and members data by keeping this secure and confidential. We will only use personal information held about others, whether employees, members, volunteers or residents, for the purposes for which it was provided and authorised, and only disclose it to those others who are entitled to see it for the same purposes.

A key objective of this Policy is to help ensure that everyone who views or handles data and information in any format as part of their duties or employment with us meets these requirements.

An appendix details how long we retain documentation to meet regulatory and other requirements.

What does this mean for me?

As a resident, we want you to be confident of the staff and volunteers who support you and aware of the requirements which are placed upon them in terms of using and handling your personal details.

As an employee, trustee or volunteer, unless specifically authorised by our Board to do so as part of your duties you may not and must not use or disclose to any other person, during or after working for or with our Society, any confidential documents, facts, information or trade secrets relating to the business or affairs of the Society or its employees, trustees, members or volunteers which come to your knowledge during your work or time with us.
Particular care must also be taken to avoid accidental disclosure of such information.
More detail is included in the Statement which forms part of this policy.

Similarly you must not make or keep any copies of electronic or paper documents or extracts that come into your possession through your work with us other than for the purpose intended in the course of your duties with us.

On termination of your involvement in any capacity with our Society, you must not take with you or keep any information about our residents, sales, suppliers, whether papers, charts, bulletins, reports, drawings, blueprints, models or any copies or extracts of these. Any and all such items belong to us and you must surrender them to us, or destroy them.

2. Social Media, Digital devices and content

Our Trustees are responsible for publication of any material relating to our society through any channel. This includes social media, and the confidentiality and data protection rules described in this policy must be observed on any matters relating to our Society in general and our residents, staff and volunteers in particular. Any Social Media sites set up in the name of the Society must be authorised by the Trustees and only those delegated to manage the sites may do so. Controversial opinions should be avoided.

The principles outlined above similarly apply to digital information held on smart phones and tablets which can store and transmit large quantities of data. Inevitably trustees, volunteers and staff will use their own equipment for both their personal and work or volunteering roles. The same attention

to data protection issues is needed when using such devices (whether Society or personally owned equipment) which may receive, access, or store data. In particular, access to the device must be password or e.g. fingerprint protected.
Mobile phones (including smart phones) tablets, computers and other equipment provided to our staff or volunteers for company use may only be used for that purpose. Costs associated with the use of company supplied items will be reimbursed through the expenses system, as will calls for company business on personally owned equipment (detailed records need to be kept).

Devices which we provide remain our property. The user agrees to the following responsibilities:

- To be accountable for the device and its use until it is returned (Unauthorised transfer of devices is not allowed)
- To exercise reasonable care for the device, avoiding damage or loss.
- To limit unnecessary mobile usage and use a landline where this is more economical.
- To use devices safely (see below)
- Not to use company phones for personal calls other than in exceptional circumstances and to pay for such calls.
- To advise if the company equipment is lost, stolen or damaged.
- To return equipment in good condition and any batteries, chargers etc when required.

At the time of publication the only such device we supply is the laptop used by the Company Secretary and basic mobile phones for our Secretary & Applications Secretary to handle external enquiries.

In practice, any corporate phone usage is likely to be only a fraction of the total time most of our volunteers and staff will otherwise spend on their own device. There is no strong evidence to suggest that mobile phone and base station emissions create a health risk, though radio frequency radiation may cause subtle health effects. There are conflicting views on excessive “screen time” and the demands of responding to calls and notifications.

When used for Society purposes, we suggest that regular breaks be taken and mobile phone calls limited to ten minutes where possible. Use of hand held electronic devices whilst driving is illegal, and under no circumstances should they be used to pick up calls, texts or emails whilst driving on company business. This includes times when stopped at traffic lights or during other holdups where the vehicle can be expected to move off after a short while. We recommend turning devices off and collecting any messages or texts when stopped at a suitable location.

3. Guidelines for collection, use and management of personal data

Those for whom we hold personal data, including residents, staff, trustees and volunteers, have the following rights
(a) the right to confirmation as to whether or not we have their personal data and, if we do, to obtain a copy of it;
(b) where technically feasible, the right to have certain information provided to them in a portable electronic format or have it transmitted to another controller;
(c) the right to have inaccurate data rectified;
(d) the right to object to their data being used for marketing or on legitimate interests grounds (including for profiling where applicable);
(e) where their data is processed on the basis of consent, the right to withdraw that consent;
(f) the right to restrict how their personal data is used; and
(g) the right to have their data erased in certain circumstances (though this may not apply if it is necessary for us to continue to use the data for a lawful reason).

Staff and volunteers who collect, process or manage personal data must comply with the following conditions to meet these rights:

- There must be a clear and foreseeable need for all personal data collected.
- Where specific personal information is sought from an individual, the individual should be informed as to the purposes for which that data will be processed and their consent obtained.
- Personal data obtained for a specified purpose should not be processed for another purpose without the individual's consent (or further consent).
- Any personal data processed should be accurate, up to date, relevant, and not excessive for the purpose for which it is collected.
- Employees and volunteers must be aware of how the data will be used.

4. Guidelines for collection, use and management of personal data

Those for whom we hold personal data, including residents, staff, trustees and volunteers, have the following rights
(a) the right to confirmation as to whether or not we have their personal data and, if we do, to obtain a copy of it;
(b) where technically feasible, the right to have certain information provided to them in a portable electronic format or have it transmitted to another controller;
(c) the right to have inaccurate data rectified;
(d) the right to object to their data being used for marketing or on legitimate interests grounds (including for profiling where applicable);
(e) where their data is processed on the basis of consent, the right to withdraw that consent;
(f) the right to restrict how their personal data is used; and
(g) the right to have their data erased in certain circumstances (though this may not apply if it is necessary for us to continue to use the data for a lawful reason).

Staff and volunteers who collect, process or manage personal data must comply with the following conditions to meet these rights:

- There must be a clear and foreseeable need for all personal data collected.
- Where specific personal information is sought from an individual, the individual should be informed as to the purposes for which that data will be processed and their consent obtained.
- Personal data obtained for a specified purpose should not be processed for another purpose without the individual's consent (or further consent).
- Any personal data processed should be accurate, up to date, relevant, and not excessive for the purpose for which it is collected.
- Employees and volunteers must be aware of how the data will be used.

5. General Data Protection Regulations (GDPR))

This and the following sections provide more detailed information for those responsible for managing and handling data. GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018) both of which apply from 25th May 2018. We will follow the letter and spirit of these provisions for all of our records to ensure conformity to these regulations.

5.1 GDPR

A self-assessment for our Society of GDPR requirements (based upon the on-line Data Protection Toolkit provided by the Information Commissioners Office) is included as an appendix to this policy together with links to the ICO site.

5.2 Data Security and Protection Principles

5.2.1 GDPR principles reiterate those described in Section 5 above, with the following definitions:

a) Personal Data is defined as data which relates to a living individual who can be identified from the data or from a combination of that data with other information in their possession, or likely to

come into the possession of the holder. Note that data does not have to be private or sensitive in order to constitute personal data and includes information such as names, addresses and telephone numbers. Personal data can cover both facts and opinions that are held about an individual. It also includes information regarding our Society's intentions towards the individual. Data relates to any information held on a computer (including e-mails) or manually held paper records that have been stored in a structured way so that information can be found easily.

b) Sensitive Personal Data is defined as information about an individual's racial or ethnic religious beliefs or other beliefs of a similar nature; trade union membership/non-membership; physical or mental health or condition; sex life; criminal or alleged criminal offences or any proceedings for an offence or alleged offence.

Disclosure of personal information outside our Society will normally only be made with the informed consent of the individual concerned. Exceptionally we may need to do so, for example:

- to comply with the law (e.g. police, Inland Revenue, Council Tax Registration Officer) or a court order.
- where there is a clear health or safety risk or evidence of fraud.
- in connection with court proceedings or statutory action to enforce compliance with tenancy conditions (e.g. applications for possession or for payment of HB direct).
- to provide the name, address and contact number of a resident to contractors or other agents providing services on the association's behalf.
- anonymously for valid statistical or research purposes, provided it is not possible to identify the individuals to whom the information relates.

5.2.2 As Registered data users, we will comply with the following Data Protection Principles:

- Personal data must be obtained and processed fairly and lawfully.
- Personal data must only be held for the lawful purposes set out in our data user's resister entry.
- Personal data must only be used for the purposes for which it was collected and it may only be disclosed to those people described in the register entry.
- Personal data must be adequate, relevant and not excessive in relation to the purpose for which it is held.
- Personal data must be accurate and up to date.
- Personal data must not be kept longer than is necessary for the registered purpose.
- Personal data must be accessible to the individual concerned, who has the right to have inaccurate information about themselves corrected or erased.
- Adequate security measures must be taken against unauthorised access, alteration, disclosure or accidental loss or destruction.

5.2.3 More specifically, our self-assessment and compliance with the security and protection principles mentioned above is based upon the following set of operational procedures and requirements.

Our registered "Data Controller" is The Abbeyfield Lytham St Annes Society Ltd .
Our nominated protection lead / information officer is our Secretary to the Company

Personal data which we currently hold includes the following:

- Personal Files and information held in paper format &/or on a computer
- List of names and addresses whether on spreadsheets or paper
- List of names and home telephone numbers
- Paper or computer based employee files containing employment records
- Training Records – including personal development plans

- Performance records
- Information received from third party benefits' providers regarding benefits choices e.g. pensions
- References provided to, or received from, external sources
- Management audit documentation
- Computer files holding names of individuals
- Emails which mention an individual's name (note that there is regular email traffic between Trustees/ Volunteers using their personal email addresses, and to a lesser extent staff. Care is taken not to include identifiable names (e.g. Resident X) should any content be of a personal nature.

This list is not exhaustive and may be subject to change.

Our Society's confidential data stored in computerised form is presently held on a single company laptop, password protected, turned on and used only for company business and normally held by the Company Secretary (or a nominated individual when absent).
Copies of this data are provided in paper rather than file format to those who need temporary access.
Such data is regularly backed up externally every day.
Non-confidential data company data (e.g. our Policies) can be accessed by authorised staff and volunteers through our network.
We have our own website, which holds no personal or business confidential information

Apart from banking records, the external providers with access to confidential data are:
the Accounting firm which also handles payroll on our behalf
our insurers in respect of death in service benefits
our pension providers.
the provider of our emergency contact arrangements
We have appropriate confidentiality agreements with these organisations.

Confidential data or important items stored in paper form are held in securely locked cabinets (e.g. historical files) or secure boxes (e.g. current resident support, needs and risk assessment forms) accessible only to those authorised staff and volunteers involved.
To ensure fairness, openness and accuracy, in general items containing personal information relating to staff, residents or volunteers is either copied to them or seen and signed at the time it is created.
We have timely systems in place to review, update and/or delete out of date and expired information.
We do not use any externally supplied confidential data e.g. for fundraising purposes.

All residents, staff and volunteers have access to all of our policies, either electronically or in paper format held at each house. It is a responsibility of both staff and volunteers to have read and be familiar and comply with the contents of this policy (and others as designated).
Whilst the contents of this policy are not contractual, following appropriate consultation we reserve the right to amend it without compensation.

d) More generally, the purposes for which we may hold and process an individual's personal data are as follows:

In relation to employment, including but not limited to :-
administering and maintaining personnel records; paying and reviewing salary and other remuneration and benefits; providing and administering benefits (including if relevant pension, life assurance and medical insurance); undertaking performance appraisals and reviews, including talent review and succession planning; dealing with performance, disciplinary, harassment and bullying, and grievance proceedings; providing references and information to future employers, and, if necessary, governmental bodies for social security and other purposes, e.g. the Inland Revenue

and the Contributions Agency; providing information to future “purchasers” should the business of the Society be closed or transferred.

Similarly in relation to trustees, volunteers and self-employed workers in relation to their work with us, including (but not limited to) administering and maintaining records of work undertaken and expenses or remuneration payable, we may hold personal data including name, address, telephone number and emergency contact, bank account details and national insurance numbers, paper or computer based files containing job content and training records, information provided to, or received from, external sources and information contained on e-mail which mentions the individual’s name. This list is not exhaustive and is subject to change.

In relation to Sensitive Personal Data our Society may process

- racial or ethnic origin for statistical monitoring purposes, in accordance with the Commission on Racial Equality guidelines.
- data on an individual’s health for the purposes of maintaining sickness or other absence records*, and taking decisions as to an individual’s fitness for work and entitlement to related benefits
- information on criminal or alleged criminal offences in order to determine suitability for continued employment, where appropriate.

*Details of work related injuries or illnesses will be reported in accordance with legal requirements.

Sensitive personal data may also be processed, in accordance with data protection legislation, to exercise or perform a right or obligation conferred or imposed on us by law in connection with employment, legal proceedings or for the purpose of obtaining legal advice, or for administration of justice.

5.2.3 Data Breaches

GDPR requires Data Controllers to notify any Personal Data Breach to the Information commissioner and, in certain instances, the Data Subject. We will do so should any suspected Personal Data Breach have occurred and will notify Data Subjects or any applicable regulator where we are legally required to do so. Any Trustees, staff or volunteers who know or suspect that a Personal Data Breach has occurred should immediately contact our Secretary or Chair. Any and all evidence relating to the potential Personal Data Breach must be preserved.

6. Rights of Access – Formal and Informal Requests

An individual may make an informal request to view a file that is held on him or her rather than a formal request to access all information. If the individual requests to see his/her personal file, it is important to ensure that he or she is only interested in viewing this file, rather than any other information held on him/her. If so, a suitable time should be arranged for the individual to view his/her file and to take copies of any documents contained within the file.

Requests by an ex-employee or other individual who has had any dealings with our Society should always be considered as a formal request. Under the Act, an individual is entitled

- to be told whether anyone in the Society is holding any of his/her personal data
- if so, to be given a description of the personal data held, the purposes for which the data is being processed and those to whom the information is/has or may be disclosed.

To make a formal request for access to all information held on an individual by the Society

- The individual should be advised to put a request in writing to our Secretary

- Our Information Officer will check to ensure that the individual is who he/she claims to be, validate his/her right to gain access to the data and consider the appropriateness of the request in line with the GDPR provisions.
- Our Information Officer will contact the appropriate individuals within our Society and, where appropriate, any external organisations, and request access to or copies of all information held on that individual within any system or manual file (e.g. printouts of computer held records, copies of paper-based records).
- The information, once collated, should be made available within 40 days, unless the burden of providing the information is excessive.

In some circumstances it may be appropriate for our Information Officer to agree an appropriate time for the individual to review the information held on file, and take copies of documents, as appropriate. Where appropriate, any inaccuracies will subsequently be amended.

7. Disclosure of information relating to another person (an additional data subject)
Where documentation relating to an individual also discloses information relating to another person (an 'additional data subject'), this will also be the additional data subject's personal data.

The following steps must be followed when deciding whether to disclose data in these circumstances

- Try to get the additional data subject's consent to disclose this information. If consent is given then the information should be disclosed.
- If consent is refused, but the feedback can be edited so as to remove all information which would identify the additional data subject, then the edited version should be disclosed.

Where consent has been refused (or cannot be obtained because the additional data subject has left our Society and cannot be traced), and it is not possible to 'anonymise' the information, we will need to decide if it is reasonable to disclose the data in any event. This will need to take into account

- was the additional data subject aware when they wrote the document that it could possibly be released
- any reasons given by the additional data subject for refusing consent to it being disclosed, whether releasing the information could actually be damaging to the additional data subject and what impact the documentation has, or might have in future, on actions or decisions relating to the individual.
- whether the feedback includes facts which the individual ought to be made aware of because he/she may dispute them and the fact that greater protection must be given to information about someone's private life than information given in a business capacity.

8. Exemptions from Disclosure
We are entitled to refuse to disclose information in the following circumstances

- Confidential references given, or to be given by us
- References supplied to us, unless the provider has consented or disclosure is otherwise reasonable in the circumstances
- Personal data processed for the purposes of management forecasting or planning, if disclosure would prejudice the conduct of the business
- Records of the employer's intention in connection with negotiations with the individual, if disclosure might prejudice those negotiations

9. Disclosure of information without informing the data subject
We are not required to notify an individual prior to disclosing information about them in the following circumstances

- Various exemptions for certain crime and taxation purposes, where compliance with the provision would be likely to prejudice the crime/taxation purpose.

- Where disclosure is required by law (e.g. requests from Inland Revenue, Child Support Agency, Benefits Agency, Department of Work and Pensions, Financial Services Authority) or a court order.

Where such disclosure is required and where practicable we will seek to obtain the request in writing and also establish the identity and authority of the person making the request for disclosure.

If someone maintains that we have a legal obligation to disclose, ensure the request is received in writing, spelling out the basis on which legal obligation is asserted. Check the assertion is valid before disclosing. Make a copy available to the individual, and give him/her a chance to check the accuracy.

Keep a record of who made the disclosure; who authorised the disclosure; the person requesting the disclosure; the reasons for the disclosure the information disclosed; and the date and time of the disclosure.
In an emergency, generally in life and death situations, the request should be made in writing, if possible, and the disclosure should be made by the Information Officer
The individual should be informed that the disclosure has been made if practicable.

10. Publication of information relating to individuals
No information should be published regarding individuals unless the individual has consented OR publication would be expected, the individual is informed in advance, their reasonable objections are respected and the information is not intrusive.

11. Appendices
The following are appended to this policy
Confidentiality & Privacy Policy Statement
Notes and Authorities for New Tenants, their Representatives and/or Family Members
GDPR Self Assessment
Document Retention and Disposal **

12. Changes since last version
Originally intended for introduction in June 2018, this policy was held back pending developments relating to GDPR. It is published for the first time in 2020 and includes content from several TAS polices (particularly in the Appendices).

APPENDIX : - **CONFIDENTIALITY AND PRIVACY POLICY STATEMENT**

Our overriding aim is to protect and promote the best interests of individuals and of the Society, and any question should be answered by reference to this principle. The Society, its staff and trustees will:-

- Treat all personal and sensitive organisational information as confidential to the Society;
- Comply with the law regarding the protection and disclosure of information;
- Not disclose personal information without the prior informed consent of the individual concerned, except in the circumstances outlined below in the section on disclosure;
- Not gain or attempt to gain access to information they are not authorised to have.

All personal information relating to residents, applicants, staff and trustees that is not a matter of public record will be:

- Obtained fairly;
- Held for specific purposes and used only for those purposes;
- Relevant, accurate and kept up to date;
- Corrected if shown to be inaccurate;
- Kept no longer than necessary and destroyed when no longer required;
- Protected against loss or disclosure;
- Treated as confidential at all times.

Any breach of this policy could have very serious consequences for an individual or for the Society and will be treated as a serious disciplinary matter.

The letter that is issued to a potential new resident will explain the reason for requiring personal information. This letter will also confirm that the data collected for one purpose will not be used (or passed to other parties) for another purpose.

Information to be kept confidential

All sensitive information will be kept and handled confidentially, whether the information has been received formally, informally or discovered by accident. Broadly, this means

- Anything of a personal nature that is not a matter of public record about a resident, applicant, staff member trustee, volunteer or society member.
- Sensitive organisational information which could be used to damage the association or threaten the security of property or buildings;
- Tenders and quotations for services and works.

Personal information may be kept in paper or computer file format. It will be stored securely – either in locked cabinets or boxes or on the Society's computer, at our registered office or in the home of our Secretary (or one of our volunteers who may temporarily be providing cover).

Access to sensitive information

Staff, trustees and volunteers will generally have access to all information that they genuinely need to know to carry out their work, and have a duty to respect the confidentiality of all personal information held by the Society. In particular, it is imperative that confidential information about a resident is not disclosed to another resident, nor should staff and volunteers gossip about residents to one another.

Wherever possible, staff, trustees and volunteers will explain the purpose of recording potentially sensitive personal information and the people likely to have access to it before it is disclosed, so that informed consent can be obtained. If this causes concern, special arrangements for recording and access will be made.

Residents in shared housing are likely to be aware of personal information about other residents and are expected to respect their right to privacy.

It is particularly important to keep secure matters referred to in minutes of meetings which may directly or indirectly make reference to individual residents or confidential plans or actions of the society.

Privacy
The letter issued to new residents will confirm that their room is private and personal to them; that they will have their own key; that they may invite visitors into their room; no one will enter their room without permission except in an emergency.

Appendix -
Notes and Authorities for New Tenants, their Representatives and/or Family Members

As a potential tenant, we will need to hold personal information about you in order to safely provide the levels of support we can offer. We may not be able to admit you as a resident without your consent to do so. The data involved includes identity evidence of your name, date of birth and right to reside in the UK and contact details of address, email and phone numbers. We do not expect to hold any bank account details for you, but our records will show your payments received each month. We also keep more sensitive information in connection with your support needs and tenancy agreement. An early objective will be to complete a "Support, Needs and Risk Assessment," usually during your trial stay at one of our houses, and you will be provided with a copy if you wish. This enables us to assess the support that you require, the acceptability of the risks involved, and whether our staff and volunteers will be able to meet your needs. Other personal information will vary on a case by case basis, for example to help us resolve breaches of tenancy, alleged anti-social behaviour or fraud.

Exceptionally we do provide contact data to an external organisation for use in emergency (currently to New Progress Housing Association Ltd who provide Call Centre cover) so that they may contact the resident and /or family friend or sponsor as authorised. We also provide regulatory information as required, for example of and for current residents at each house to the TV licencing authority each year to enable collective TV licence renewal. The organisations involved may change from time to time.

We regard all personal data as confidential and take care to use it only for the purpose for which it is held. Most is collected in paper format, but will be converted to computer copies or files. Where paper is retained, it is filed securely and can only be accessed by those with the appropriate codes or keys. Our centrally computerised data is currently held on a single laptop and backed up to "cloud storage," again accessible only by those with an appropriate security code. The personal information we collect is only shared with staff and volunteers appropriate to the purpose for which they are employed or serve with us. It may be accessed remotely or sent via email to them, but will not be intentionally transmitted outside the UK or passed to other organisations. In particular we do not use your data for marketing purposes, or sell, rent or pass it on to third parties. We will write to you from time to time with regard to your tenancy and other matters relating to the house and society.

With the authority of each resident, we may also share their personal details with named family, friends or representatives. Our staff and volunteers may similarly share concerns or pertinent information with the same named individuals in emergency or where we consider that there has been a significant change in the condition of the resident which has affected their health or welfare. Also in the event of an emergency, we may share medically related information with the emergency services or agencies which become involved.

You have the right to request a copy of the information we hold about you. If you would like a copy of this information, please write to the Data Controller at the address in the heading or email abbeyfield.lsa@btinternet.com.You may ask us to correct or erase any data that you think is inaccurate. We also want to be sure that any personal information we hold on you is accurate and up to date, so please keep us informed of any future changes. Data will only be retained for as long as it is needed in relation to the purpose for which it was collected, and full details are included in our Data Confidentiality, Privacy,Protection & Retention Policy, a copy of which is available at the house, on our website, or can be provided on request.

…….continued on next page

Our Society provides “independent living” in sheltered accommodation. Maintaining independence and dignity and encouraging our residents to be as active and involved as possible are important principles for us. We do not and cannot provide nursing or medical care and are not CQC registered or regulated to do so. Though we cannot care for our residents, we do care about them and want to offer the best support that we are able and legally permitted to provide. A key purpose of this note is to ensure that, as a new resident, their representative or a family member, you fully understand the limitations of the service we will be able provide and acknowledge the boundaries that we need to maintain and fall within.

Whilst there is often an employee or volunteer on our premises, our staff are only employed for a limited number of hours each day and are not therefore generally available and “on-call” outside of their working time. They can be contacted whilst on duty to assist and support residents and will be pleased to help. Our volunteers may also become involved where appropriate.

Not all emergencies require a medical response and not all medical problems are emergencies. Our staff or volunteers may be able to help in organising assistance in less urgent situations, but the response service that we offer for emergencies is based around use of pendants - linked to each tenant’s telephone land-line - which should be worn or kept close and accessible at all times. Using the pendant alerts a call-centre. They have contact details for each resident (and in some cases of a family member or representative) and activate the following sequence
: attempt to call the resident to check the call is not accidental, and if possible what is wrong.
: attempt to call the Duty Manager and get them to check on the resident if they are available.
: call any nominated family member or representative who lives locally and is in a position to check.
If no response to these steps then alert emergency services and send a paramedic.

There will almost always be a “Duty Manager” who is resident or sleeping-in at the house, but they may be out during the daytime or evening, or otherwise occupied, should an emergency occur. If the manager is available and able to respond and assist when alerted by the call-centre they will do so, and then update the call-centre on the situation. The call-centre or the manager will then summon appropriate help. The manager may be able to stay with and comfort the resident until help arrives, but this is not guaranteed. They may also be able to provide emergency first aid, but for the reasons explained above are not there to provide medical or nursing help. They will not be able to accompany the resident in an ambulance or follow them to hospital.

If, when a Duty Manager becomes involved, the resident says that they do not need an emergency response - e.g. that they do not wish to be taken to Casualty – then the manager will accept their decision unless they are of the view that the resident may be confused and/or not in a position to think clearly or understand the potential seriousness of any medical issues. Similarly they will accept the resident’s instructions with regard to contacting family or other representatives at that time. It will be for the manager to exercise appropriate discretion in such situations, but with the aim of respecting the wishes and dignity of the resident whenever reasonably possible.

In order to determine the day to day support required by each resident and also for any emergency process which may arise, we keep and maintain personal data – primarily the Support, Needs and Risk Assessment described above - for use by our staff and volunteers, and also the call-centre and any personnel who may be involved in a medical or emergency response. This may include details of medication and contact details for family or other representatives who have agreed to be involved in such situations. For clarity, and in order to meet requirements under the General Data Protection Regulations (GDPR), we therefore seek specific assent for the data involved to be held used in this way and for this purpose. It is for the resident to decide which family member or members and/or other representatives are to be involved in the processes described above and the extent of their involvement. Each should therefore authorise acceptance of this note and the part they may play in the circumstances described by signing copies of this note - retaining one for their own records and returning the other for us to keep on our files.

This page to be completed by the Potential Resident

I confirm that the personal data you hold for me may be used and provided for the specific purposes described above relative to my capacity as a resident. I further confirm that I understand and accept the processes described in this note and the limitations and boundaries of the available support which may be involved.

I wish to nominate the following person or people in the capacity indicated:

Representative to assist and support me as appropriate and also to act for me in the event that I am incapacitated and unable to make my own decisions at some future point (note that this does not constitute power of attorney for any matters requiring legal authority)

……

List of family member(s) &/or friends to be contacted in the event of emergency

……

……

……

Signed **……..**

Name (please print)… **……**

Date……..

This page to be completed by each named representative & / or family member.

I confirm that the personal contact data you hold for me may be used for the specific purposes described above relative to my capacity as a representative &/or family member.

I further confirm that I understand and accept the processes described in this note and the limitations and boundaries of the available support which may be involved.

In particular, I wish and agree

- ☐ **to be contacted and involved as part of any emergency process where possible** (for example this could include travelling in an ambulance or meeting up at hospital)

- ☐ **to be notified as soon as possible (day or night) when an incident has occurred OR**
- ☐ **to be notified during the working day on or following an incident**

Signed……..
Relationship: Representative / Family member

Name (please print)……..
Date……..

Appendix:
ICO – (Information Commissioners Office) - Self Assessment of GDPR requirements

NB See https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment **for the latest version**

Items		Not yet implemented or planned	Partially implemented or planned	Successfully implemented	Not Applicable
Step 1: Data protection policy, responsibility and training. Our business					
1.1 Policy	has established an appropriate data protection policy.			*	
1.2 Management responsibility	nominated a data protection lead.			*	
1.3 Training and awareness	provides data protection awareness training for all staff.			*	
Step 2: Registration, privacy notices and subject access. Our business					
2.1 Registration	has registered with the Information Commissioner's Office.			*	
2.2 Privacy notices	has made privacy notices readily available to individuals.			*	
2.3 Responding to subject access requests	has established a process to recognise and respond to individuals' requests to access their personal data.			*	
Step 3: Data quality, accuracy and retention. Our business					
3.1 Data quality and accuracy	has established processes to ensure personal data is of sufficient quality to make decisions about individuals.			*	
3.2 Retention and disposal	has established a process to routinely dispose of personal data that is no longer required in line with agreed timescales.			*	
Step 4: Security. Our business					
4.1 Security policy	has established an information security policy supported by appropriate security measures.		*		
4.2 Outsourcing	ensures an adequate level of protection for any personal data processed by others on your behalf or transferred outside the European Economic Area.			*	
Step 5: Privacy impact assessments. Our business					
5.1 Privacy Proofing	has established a process to ensure new projects or initiatives are privacy-proofed at the planning stage.		*		

Appendix: Document Retention and Disposal – Short Version
When no longer required, all personal information will be safely shredded or destroyed.
Note that retention periods for certain types of information are laid down in regulatory body guidelines. Those for our Society are as follows:

Document	**Retention Period**	**Document**	**Retention Period**
GOVERNANCE		**RESIDENTS**	
Register of Board Members/Directors	Permanently	Application Records	6 years
Register of Seals : Register of Share Certificates	Permanently	Rent Statements	2 years
Organisation charts	6 years	Care Resident files	Indefinitely
Audited Annual Accounts	Indefinitely (statutory)	Confidential files for former residents	3 - 5 years
		(former) Tenants Agreement and details of leaving	6 years
		Care/Support Plans and supporting documents	6 years
STAFF		**PROPERTY**	
Employee Tax Records and Pensions	6 Years (Statutory)	Property Records	12 years after interest in property ceases (Statutory)
Payroll Records	7 Years (Statutory)	Property Maintenance Records	6 years
Staff Personnel Records Including complaints/grievances	7 years after employment ceases	Invoices	7 years
Medical Records (staff)	30 years after employment ceases	Supplier contracts	6 years after contract is terminated
Copy pay slips	2 years	Accident Reports	Indefinitely

Appendix - DOCUMENT RETENTION AND DISPOSAL (Long version)

The following schedules contain recommended retention periods determined in accordance with relevant legislation, regulations and best practice, including the following which apply in England and Wales:

Key to statutory retention sources

CA – Companies Act 2006
Ch A – the Charities Acts including the Charities Act 2011
CAWR – Control of Asbestos at Work Regulations 2012
CCBS – Co-operative and Community Benefit Societies Act 2014
CQC – Outcome 21 of the Care Quality Commission's Essential Standards of Quality & Safety (N/A)
DPA – Data Protection Act 1998
EA – Equality Act 2010
IT(E)R – Income Tax (Employment) Regulations 1993
LA – Limitations Act 1980/ Limitations for legal proceedings
RIDDOR – Reporting of Injuries, Diseases & Dangerous Occurrences Regulations 2013
RBS(IP)R – Retirement Benefits Schemes (Information Powers) Regulations 1995
SMPR – Statutory Maternity Pay (General) Regulations 1986 (as amended)
SPAPR – Statutory Paternity Pay & Statutory Adoption Pay (General) Regulations 2002 (as amended)
SSPR – Statutory Sick Pay Regulations 1982 (as amended)
TMA – Taxes Management Act 1970
VATA – Value Added Tax Act 1994

N.B. Where the Statutory and Recommended Retention Periods differ, the Recommended Period should be used

Document	Statutory Retention Period : Source		Recommende Retention	Comments
1.GOVERNANCE DOCUMENTS				
Certificate of Incorporation	N/A	N/A	Permanently	Implied by CA, Sec.15.
Certificate of change of company name	N/A	N/A	Permanently	Implied by CA, Sec.80.
Memorandum and articles of association (original)	N/A	N/A	Permanently	Best practice
Articles of Association (current)	Permanen tly	CA	Permanently	Best practice
Constitution, Aims and objectives	N/A	Ch A	Permanently	Required for charitable status
Confirmation of charitable registration	N/A	Ch A	Permanently	Best practice

HMRC Confirmation of charitable status	N/A	N/A	Permanently	Best practice
Registration documentation (Registered societies formerly Industrial & Provident Societies)	Permanently	CCBS	Permanently	Best practice
Certificate of registration with the housing regulator	N/A	N/A	Permanently	Best practice
Board member documents – apt letters, SLAs, bank details etc	N/A	N/A	6 years after board membership ceases, some details should be destroyed when membership ceases e.g. bank details	DPA - 5th principle * CA - recommendation for docs post termination of directorship
Register of trustees, directors and secretaries.			Permanently	
Register of Trustees' Interests			Permanently	
Documents regarding Society Membership (including correspondence).			In general, for the duration of the membership plus 6 years. There may be occasion to weed very old, but still current, files. Any live issues must be kept.	
Complaints files			Date of resolution of complaint plus 6 years.	
Whistleblowing investigation files			Date of resolution of issue plus 6 years.	
Policies & Procedures			Retain current version and	

			previous version for 3 years.	
2. MEETINGS (INCL AGMs)				
Notices of meetings	N/A	N/A	6 years	In case of challenge to validity of meeting or resolutions.
Board and committee minutes (including agenda's & reports)	Permanently	CA & ChA	Permanently	Signed originals must be kept. Charity Commission requirement CC48
Board resolutions	Permanently	CA & ChA	Permanently	Signed originals must be kept. Charity Commission requirement CC48
Executive Committee Minutes and papers	N/A	N/A	Permanently	Signed originals must be kept
3. REGISTRATIONS AND STATUTORY RETURNS:				
Annual returns to the regulator	N/A	N/A	5 years	Best practice
Audited company returns and financial statements (including Registered Societies' (formerly I & P Societies') Annual Returns to Registrar of Friendly Societies(FCA))	N/A	N/A	Permanently	Best Practice
Declarations of Interest	N/A	N/A	6 years	Limitation for legal proceedings
Register of directors and secretaries	Permanently	CA	Permanently	
Register of Shareholding members	Permanently	CA	Permanently	Records may be removed from register 20 years after membership ceases.
Register of seals	N/A	N/A	Permanently	Best practice
Register of share certificates	N/A	N/A	Permanently	Best practice
List of members (Registered Societies' (formerly I & P Societies))	N/A	N/A	Permanently	Required by Registrar of Friendly Societies (FCA)
4. STRATEGIC MANAGEMENT				
Business plans & supporting documentation (e.g. organisation structures, aims, objectives, funding issues)	N/A	N/A	5 years after plan completion	Best practice
Audit records (internal & external)			6 years from completion of	Best practice

			audit	
Audit reports (internal & external)			6 years from completion of audit	Best practice
5. INSURANCES				
Current and former policies	N/A	N/A	Permanently	Limitation can commence from knowledge of potential claim and not necessarily the cause of the claim. N.B. Housing Association Boards must annually reaffirm formally their continuation of the Voluntary Board Members Liability Policy (automatically provided via NHF membership). NCVO recommends 3 years after lapse.
Annual Insurance Schedule	N/A	N/A	6 years	Best practice
Claims and related correspondence	N/A	N/A	2 years after settlement	Zurich Municipal recommendation. NCVO recommends 3 years after settlement.
Indemnities and guarantees	N/A	N/A	6 years after expiry	Limitation for legal proceedings. 12 years if related to land.
Employer's liability insurance certificate	N/A	N/A	40 years	2008 regs removed requirement to retain for 40 years but need to be mindful of 'long tail' industrial disease claims etc
6. FINANCE, ACCOUNTING & TAX RECORDS				
Accounting records for Limited Company	3 years form the date made	CA sectio n 388	6 years	TMA Section 20 may require any documents relating to tax over 6 (plus) years.
Accounting records for Registered Society (formerly I & P Society) or Charity	N/A	N/A	6 years	Required by Registrar of Friendly Societies (FCA) and Charity Commission.
Balance Sheet and Support Documents	N/A	N/A	6 to 10 years	Best practice. To relate to accounting records.
Loan account control reports	N/A	N/A	6 years	Best practice
Social Housing Grant Documentation	N/A	N/A	Permanently	Best practice
Signed copy of report and accounts	N/A	N/A	Permanently	Best practice
Budgets and internal financial	N/A	N/A	2 years	Best practice

reports				
Tax returns and records	N/A	N/A	10 years	TMA s.20. may require any documents relating to tax over 6 (plus) years
VAT records	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Orders and delivery notes	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Copy invoices	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Credit and debit notes	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Cash records and till rolls	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Journal transfer documents	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Creditors, debtors and cash income control accounts	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
VAT related correspondence	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
7. OTHER BANKING RECORDS				
Cheques	N/A	N/A	6 years	Limitation for legal proceedings
Paying in counterfoils	N/A	N/A	6 years	Limitation for legal proceedings
Bank statements and reconciliations	3 years from the end of the financial year the transact's were made	CA	6 years	Limitation for legal proceedings
Instructions to bank	N/A	N/A	6 years	Limitation for legal proceedings
8. CONTRACTS AND AGREEMENTS:				
Contracts under seal and/or executed as deeds	N/A	N/A	12 years after completion (including any defects liability period)	Limitation for legal proceedings.

Contracts for the supply of goods or services, including professional services	N/A	N/A	6 years after completion (including any defects liability period)	Limitation for legal proceedings (12 years if related to land)
Documentation relating to small one off purchases of goods and services, where there is no continuing maintenance or similar requirement	N/A	N/A	3 years	Best practice. Suggested limit: goods or services costing up to £10,000.
Loan agreements	N/A	N/A	12 years after last payment	Best practice
Licensing agreements	N/A	N/A	6 years after expiry	Limitation for legal proceedings
Rental and hire purchase agreements	N/A	N/A	6 years after expiry	Limitation for legal proceedings
Indemnities and guarantees	N/A	N/A	6 years after expiry	Limitation for legal proceedings
Documents relating to successful tenders	N/A	N/A	6 years after end of contract	Best practice
Documents relating to unsuccessful tenders	N/A	N/A	2 years after notification	Best practice
Forms of tender	N/A	N/A	6 years	Best practice
9. FUNDRAISING & MARKETING				
Deeds of covenant	6 years after last payment	TMA	12 years after last payment	Limitation for legal proceedings if related to land
Donations granted and related correspondence	N/A	N/A	6 years	Best practice
Gift Aid Declarations & Claims			6 years from the end of the tax year in which the last payment under the declaration was made.	
Legacies records including related correspondence and			6 years after the Estate	Limitation

copy Wills.			has been wound up (subject to the terms of any restrictions affecting when/how the legacy can be used).	
Consent to direct marketing		DPA	Until data preference changed	
Consent for the processing of personal data		DPA	For as long as the data is processed and held in respect of living individuals	
Image Consent forms			6 years after the consent is no longer needed.	Best practice & Limitation.
Raffle tickets		Gambling Commission	3 years from the end of the tax year	
Sponsor forms			6 years from the end of the tax year	
Marketing leaflets and brochures			6 years after the leaflet or brochure has ceased to be used.	Limitation
Press releases			6 years	Limitation
10. APPLICATION AND TENANCY RECORDS:				
Applications for accommodation	N/A	N/A	6 years after offer accepted	Best practice
Continuous recording of lettings and sales (CORE) data record form	N/A	N/A	None	Best practice in DPA compliance requires form to be destroyed immediately statistics have been recorded

Housing benefit notifications	N/A	N/A	2 years	Recommendation of Institute of Rent Officers (now merged with CIoH)
Rent statements	N/A	N/A	2 years	Best practice
Tenants' tenancy files, including rent payment records, and details of any complaints and harassment cases	N/A	N/A	In general, for the length of the tenancy plus 6 years post tenancy. There may be occasions to weed very old, but still current, files. Any live issues must be kept.	LA and best practice with DPA compliance 5th principle *. For rent payment details, best practice suggests live system holds 2 years records plus current year.
Supporting people – subsidy claims / support plans / single assessments including supporting information			Duration of tenancy	
Former tenants' tenancy agreements, and details of their leaving	N/A	N/A	6 years	Best practice with DPA compliance 5th principle *
Records relating to offenders, ex-offenders and persons subject to cautions	N/A	N/A	While tenancy continues	Information held on 'need to know' basis. Police sourced records may be confidential, to be dealt with as required by police.
11. RESIDENT RECORDS:				
Resident meeting minutes	N/A	N/A	One year	DPA
Residents cash and property registers/records (cash/property handed in for safekeeping)			6 years after the end of the financial year in which the cash/property was disposed of or 6 years after the register was closed.	
12. PROPERTY RECORDS:				
Rent registrations (superseded)	N/A	N/A	6 years	6 years if it has been superseded by a subsequent registration.

Rent Registration (not superseded)	N/A	N/A	Permanently	When no new fair rent has been registered (for example because there is no longer a Rent Act tenant in the property) the maximum recoverable rent will be applicable if a rent Act tenant is ever moved into the property.
Fair rent documentation	N/A	N/A	6 years	Rent Officer recommendation
Leases and deeds of ownership	N/A	N/A	While owned. Deeds of title – permanently or until property disposed of. Leases – Fifteen years after expiry (from NCVO)	Best practice
Copy former leases	N/A	N/A	12 years after settlement of all issues	Limitation for legal action relating to land or contracts under seal
Wayleaves, licences and easements	N/A	N/A	12 years after rights given or received cease	Limitation for legal action relating to land or contracts under seal.
Abstracts of title	N/A	N/A	12 years after interest ceases	Limitation for legal action relating to land or contracts under seal.
Planning and building control permissions	N/A	N/A	12 years after interest ceases	Limitation for legal action relating to land or contracts under seal
Searches	N/A	N/A	12 years after interest ceases	Limitation for legal action relating to land or contracts under seal.
Property maintenance records	N/A	N/A	6 years	Limitation for legal action.
Reports and professional opinions	N/A	N/A	6 years	Limitation for legal action relating to land or contracts under seal.
Development documentation	N/A	N/A	12 years after settlement of all issues	Limitation for legal action relating to land or contracts under seal.
Invoices	6 years	VATA	12 years	Limitation for legal action relating

				to land or contracts under seal.
VAT documentation	See Finance, Accounting & Tax Records section	See Finance, Accounting & Tax Records section	See Finance, Accounting & Tax records section	See Finance, Accounting & Tax Records section
Insurance	See Insurances section	See Insurances section	See Insurances section	
14. CAPITAL ASSETS:				
Capital Assets (other than property)	N/A	N/A	Date of purchase to at least 6 years after date sold, transferred or disposed.	
Fixed Asset Register	CA and Ch A	N/A	Permanently	
15. EMPLOYEES: TAX AND SOCIAL SECURITY				
Record of taxable payments	6 years	TMA	6 years	Inland Revenue require retention of each payment record for 3 years
Record of tax deducted or refunded	6 years	TMA	6 years	Inland Revenue require retention of each payment record for 3 years
Record of earnings on which standard National Insurance Contributions payable	6 years	TMA	6 years	Inland Revenue require retention of each payment record for 3 years
Record of employer's and employee's National Insurance Contributions	6 years	TMA	6 years	Inland Revenue require retention of each payment record for 3 years
NIC contracted-out arrangements	6 years	TMA	6 years	
Copies of notices to employees (e.g. P45, P60)	6 years plus current	TMA	6 years plus current year	

	year			
Inland Revenue notices of code changes, pay & tax details	6 years	TMA	6 years	
Expenses claims	N/A	N/A	6 years after audit	Best practice
Record of sickness payments	3 years following year to which they relate	SSPR	6 years	Inland Revenue require retention of each payment record for 3 years
Record of maternity, paternity & adoption payments	3 years following tax year to which they relate	SMPR & SPAPR	6 years	Inland Revenue require retention of each payment record for 3 years
Income tax PAYE and NI returns	3 years following year to which they relate	IT(E)R	6 years	Best practice
Redundancy details and record of payments and refunds	N/A	N/A	12 years	Chartered Institute of Personnel and Development (CIPD) recommendation
Inland Revenue approvals	N/A	N/A	Permanently	CIPD recommendation
Annual earnings summary	N/A	N/A	12 years	Best practice
16. EMPLOYEES: PENSION SCHEMES				
Actuarial valuation reports	N/A	N/A	Permanently	CIPD Recommendation
Detailed returns of pension fund contributions	N/A	N/A	Permanently	Best practice
Annual reconciliations of fund contributions	N/A	N/A	Permanently	Best practice
Money Purchase Details	N/A	N/A	6 years after transfer or value taken	CIPD Recommendation
Qualifying service details	N/A	N/A	6 years after transfer or value taken	CIPD Recommendation
Investment Policies	N/A	N/A	12 years from end of benefits payable	CIPD Recommendation

			under policy	
Pensioner Records	N/A	N/A	12 years after benefits cease	CIPD Recommendation
Records relating to retirement benefits	6 years after year of retirement	RBS(IP)R	6 years after year of retirement	Statutory requirement
17. EMPLOYEES (PERSONNEL PROCEDURES)				
Terms and Conditions of service, both general terms and conditions applicable to all staff and specific terms and conditions applying to individuals	N/A	N/A	6 years after last date of currency	Limitation for legal proceedings
Service contracts for Directors (companies)	3 years	CA	6 years after directorship ceases	Best Practice
Remuneration package	N/A	N/A	6 years after last date of currency	Limitation for legal proceedings
Former Employees Personnel files	N/A	N/A	6 years after end of employment.	CIPD recommendation
Appraisals	N/A	N/A	6 years after end of employment.	Best practice
References to be provided for former employees	N/A	N/A	20 years or until former employee reaches age 65 (whichever comes first)	Best practice
Training programmes	N/A	N/A	6 years after completion	Best practice
Individual training records	N/A	N/A	6 years after employment ceases	CIPD recommendation
Application forms and interview notes of unsuccessful candidates	3 months after notification	EA	1 year	CIPD recommendation LA – 1 year limitation for defamations. Successful job application documents will be transferred to

				the personnel file.
CRB (now DBS) clearance documentation	Date of clearance + up to a maximum of 6 months		Date of clearance + up to a maximum of 6 months	DBS check code of practice (Home office). Evidence of completed check (not details of the result) should remain on permanent record.
Time cards/sheets	N/A	N/A	2 years after audit	CIPD recommendation
Duty rotas/rosters i.e. organisation or departmental rosters, not the ones held on the individual's record.			4 years after the year to which they relate.	
Trade Union agreements	N/A	N/A	10 years after ceasing to be effective	CIPD recommendation
Trust deeds, rule and minutes (for joint employee/employer sports/social clubs etc, set up under trust)	N/A	N/A	Permanently	CIPD recommendation
Employer/employee committee minutes	N/A	N/A	Permanently	CIPD recommendation
Insurance claims	See Insurances	See Insurances	See Insurances section	See Insurances section
Sickness records	Three years after the end of each tax year for Statutory Sick pay purposes	SSPR	6 years from end of sickness	Limitation for legal proceedings. NCVO recommends 3 years. However for industrial injuries not detectable within that period e.g. asbestos, the time period may be extended. Also, for employees exposed to hazardous substances.
18. VOLUNTEERS:				
Volunteer files			The duration of the volunteering period plus 1 year.	So that references can be provided.
19. HEALTH & SAFETY				
Medical records relating to control of asbestos	40 years	CAWR	40 years	

Health & Safety assessments	N/A	N/A	Permanently	CIPD recommendation and best practice
Health & Safety policy statements	N/A	N/A	Permanently	Good practice
Records of consultations with safety representatives	N/A	N/A	Permanently	CIPD recommendation and best practice
Accident records, reports	3 years after date of settlement	RIDD OR	6 years after date of occurrence	Limitation for legal proceedings, DPA
Accident books	N/A	N/A	6 years after date of last entry	Limitation for legal proceedings
Health & Safety statutory notices	N/A	N/A	6 years after compliance	Limitation for legal proceedings

General points

Electronic Records and email

All electronic data should be contained in a robust filing system to allow it to be kept secure, accessed and destroyed as appropriate. All emailed information can be called upon as evidence. Any important information sent by email should be included as an attachment, not in the body of the email so it can be appropriately stored

* Disposal

Information on identifiable living individuals should not be kept for longer than is necessary for the purposes for which it was obtained and processed In practice, it means that you will need to:

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.