RECORDS MANAGEMENT POLICY	
Policy Number	GCS 2.24 Version 2.0
Prepared by	Clare Ruxton, Corporate Services Manager
Date of Review	-
Date of Next Review	October 2022
Reviewed & Approved by	Corporate Service Committee
Date	November 2019

OSPREY GROUP RECORDS MANAGEMENT POLICY

POLICY STATEMENT

Osprey Housing and Osprey Housing Moray (referred to as the Group) believe that effective and efficient management of data and information is vital to the success of maintaining good quality services for all our tenants and providing value for money.

We embrace robust data management and this is encompassed in our Core Values:

- ✓ **AMBITION**
  empowering through innovation and challenge
- ✓ (E)**QUALITY**
  doing the best for individuals and communities in a fair and equal way
- ✓ **RESPECT & PROFESSIONALISM**
  towards each other, the people we work with; the people we serve and our environment
- ✓ **ACHIEVEMENT**
  delivering outcomes that matter and make a real difference – now and in the future

Osprey Housing Group
Data and Information Management Policy and Procedure

1. Introduction

As an organisation, Osprey Housing Group manages a significant amount of data and information. Much of this data and information is sensitive personal information relating to our team members and tenants. Therefore it is essential that all staff and volunteers within the organisation are aware of the importance of managing this data and information effectively and carry out their responsibilities in this respect.

The purpose of this document is to outline Osprey Housing Group's policy and procedures for the management of data and information and consequently to give staff and volunteers guidance on the effective management of data and information.

1.1 Why should Osprey Housing Group Manage and Protect Data Effectively?

The underlying principle of records management is to ensure that records are managed throughout their life-cycle from the point they are created or received, through maintenance and use, to the time they are destroyed or permanently preserved as archival records. This is because:

- It is a legal requirement (Data Protection Act 1998 and Human Rights Act 1998)
- It is essential that we respect the rights of our tenants and staff and that they can trust us to manage and protect their information effectively.
- It makes good sense, for example:
  - Sending out mailing from incorrect or out of date records wastes time and money.
  - Good information handling enhances the organisation's reputation by increasing stakeholder and employee confidence.
  - Good information handling reduces the risk of a complaint being made against the organisation.
- If an individual suffers damage as a result of the organisation not working in line with data protection requirements, that individual may seek compensation for the damage through the courts.

1.2 What happens if Osprey Housing Group does not Manage and Protect Data Effectively?

The following may occur:

- Tenant or staff information could be lost, destroyed or used inappropriately.
- Osprey's reputation could be badly damaged.
- Osprey's finances could be affected.
- The Information Commissioner could take enforcement action against the organisation to bring processing into compliance with the principles of the GDPR, this could mean a fine for Osprey.

- An individual may seek compensation through the courts for any damage suffered.

1.3 Policy Statement

Osprey Housing Group is committed to ensuring that all data and information within the organisation is managed efficiently particularly in relation to sensitive staff and tenant information. We are committed to complying with all legislation relating to the management of data and information. All Osprey Housing staff and volunteers have a responsibility to ensure that data and information is managed effectively within the organisation.

2. Good Information Handling

2.1 Osprey Housing Group Data and Information Management Standards

This policy applies to the management of records in whatever format or media they are held which are used in the furtherance of the business activities of the Osprey Housing Group. It includes, although is not limited to: Correspondence, documents, presentations, spread sheets, data bases, social media blogs, emails, diaries, faxes, promotional/instructive/educational material, reports, website content, forms, audio and video recordings, photographs and physical samples.

In managing this data we will comply with the following standards:

- All data and information that we hold regarding staff or tenants should be collected fairly within legal requirements.
- All data and information that is collected and held regarding an individual should be relevant to the purpose and should not be excessive or irrelevant.
- All data and information held should be arranged in a structure that will enable quick and easy retrieval of information.
- All data and information that we hold regarding staff or tenants, hard copy or electronic copy, should be stored securely as per policy and procedures.
- A clear desk policy should be implemented in both Osprey offices, desks should be cleared at the end of the working day and any sensitive information should be locked away.
- Storage of current and archived data and information held within offices should be clean, tidy, clearly labelled to prevent any damage to records.
- Access to tenant and staff information should be on a "need to know" basis e.g. a key worker will require to access to information regarding a tenant that they are supporting but the administrator may not require access to this information.
- Equipment for storing data and information should prevent unauthorised access and meet fire and health and safety requirements.
- We should only share staff or tenant information with third parties on a 'need to know' basis and where we have consent from the individual. There are exemptions to this which are detailed in this policy.
- Osprey has a process in place to allow tenants to access information held about them. Staff would contact Corporate Services if they require advice and if they want to access their own information. There are exemptions where Osprey can

refuse access – these are detailed later in section 3.3 – Where Permission is not Required.

- All data and information stored regarding an individual should be accurate and up to date.
- Data and information regarding an individual should not be kept longer than necessary (See Retention Guidelines in the Osprey Privacy Policy Appendix 1)
- All departments should review data and information held on individuals on an annual basis and archive/destroy where appropriate.
- Information and data should be archived securely and within timelines as per the policy and procedures
- The destruction of data and information should be done securely as per policy and procedures.

2.2 Eight Principles of Good Information Handling

All team members handling 'personal data' must follow the eight data protection principles. The first five principles establish general standards of data quality. They specify that data must be:

1. Obtained and processed fairly and lawfully.
2. Held only for specific and lawful purposes and not processed in any matter incompatible with those purposes.
3. Relevant, adequate and not excessive for those purposes.
4. Accurate and where necessary kept up to date.
5. Not kept for longer than is necessary.
6. Processed in accordance with the rights of data subjects under this Act. This means that individuals have the right, amongst other things to;
   - be informed upon request of all the information held about them by a particular data controller.
   - prevent the processing of their data for the purposes of direct marketing.
   - be compensated if they can show that they have been caused damage by any contravention of the Act.
   - the removal or correction of inaccurate data held about them.
7. Adequately secure so that precautions are in place to prevent the loss, destruction or unauthorised destruction of the data.
8. Non-transferable outside the European Economic Area unless satisfied that the country in question can provide an adequate level of security for that data.

3. Operational Procedures

3.1 Dealing with Breaches

Osprey Housing has a Personal Data Breach Procedure GCS 2.16.2 which covers this issue.

3.2 Consent - Sharing Records and Information with External Agencies

Tenant Information - Permission from the individual is needed in some cases before their information can be shared with external agencies. Information regarding a tenant must not be shared if they have not given permission to share it with that specific

individual/agency or if they have specifically stated that they do not want information shared with a particular individual or agency. Please note for the purposes of the data protection legislation any subsidiary of Osprey is considered as an external agency and consent is required.

Staff Information – The information and records regarding our staff are held for Osprey use only and should only be accessible to other Osprey team members on a 'need to know' basis. Osprey Housing Group does not have overarching permission from our team members to share records and information with external agencies, therefore if a request is made, written permission from the team member to allow the specific information requested to be shared with that particular agency or organisation is required for each occasion.

3.3 Where Permission is Not Required

Permission to share information is not required for staff or tenants in the following circumstances:

- Where there is an obligation to report a crime.
- Where there is a serious risk of suicide, violence or abuse, especially to a child or young person.
- Where disclosure is legally required (statute or court).
- Where urgent medical attention is required.
- Where considerations of public interest outweigh other considerations.

If any of the above apply, the authority requiring the information should complete a written document confirming that they have requested this information giving documented proof of the information being taken away or shared.

3.4 Access to Records

Osprey Housing has a Data Subject Access Procedure GCS 2.16.1 which covers this issue.

3.5 Protective Marking

Protective markings will be applied to any papers which are confidential – Definitions of how Osprey categorises our documents can be found in our Data Handling Procedure GCS 2.16.4. Protective markings should be applied using either a header, footer or a watermark – using these procedures will ensure the protective marking is applied to each page. Protective markings should be applied to documents where if the information from the document was compromised it would:

- release private information about a team member or tenant.
- cause unnecessary distress to team members or tenants.
- have an impact on the operations of the business.
- adversely affect Osprey's reputation.
- impede effective communication with our tenants.

Papers which are marked confidential should be treated as such by all staff and should be shared with internal colleagues only on a need to know basis. Care should be taken with requests for sight of confidential papers from external sources and the advice of the Corporate Services team should be sought in all instances.

3.6 Electronic Data and Information

The principles for the management of electronic records are the same as those for the management of manual records. All data management standards detailed in section 3 apply to electronic records. Effective electronic record keeping requires:

- A clear understanding of the nature of electronic records.
- The establishment and maintenance of a structure of folders to reflect logical groupings of records.
- The secure maintenance of the integrity of electronic records e.g. password protected systems and access levels.
- The accessibility and use of electronic records for as long as required (which may include their migration across systems).
- The application of appropriate disposal procedures, including procedures for archiving.
- The ability to cross reference electronic records to their paper counterparts in a mixed environment. This is particular important in relation to tenant and staff records.

3.6.1 Smart Phones

As e-mails sent or received can often contain personal information about an individual or other information deemed private and confidential, it is essential that all smart phones are password protected and that only the user has the password.

3.6.2 Scanning

All of our photocopiers now have scanning facilities, scanning documents and e-mailing them is an effective way of sending information externally and reducing postage costs and paper usage.

3.6.3 Links

We have the internal facility to send embedded links to documents rather than send them as attachments by email and we should do so wherever possible.

3.6.4 Faxing

Personal information should not be sent by fax, the scanning facilities should be used wherever possible. If there is no other option, the person receiving the fax should be contacted and advised to stand by the fax machine to retrieve the document and to phone back to confirm receipt. However, this should be avoided if possible.

3.7 Storage of Data

All data and information should be stored appropriately and the following should apply to both electronic and hard data and information:

- Clear and logical filing systems and structures should be in place to store both electronic and paper based information and to assist with its retrieval.
- Paper based data and information should be stored in a clean, dry area in order to prevent any damage to files.
- Personal data and information regarding an individual should be stored in a locked filing cabinet. Access levels should be on a need to know basis and should be restricted appropriately.
- Information stored should be reviewed on a regular basis to ensure that it is up to date, accurate and still relevant for the purpose it is required for. We should not be keeping information that is incorrect, out of date or that we no longer require.
- Where possible, only current data and information that is in use should be stored in the office or electronic folders. All other paper based data and information should be archived. Electronic data and information not in use should be stored in an PC archive facility. This ensures that team members are not dealing with vast quantities of information and can easily access current information. In relation to paper based information it ensures that office spaces are kept tidy.
- All staff should ensure that paper based data and information is filed on a regular basis, that personal data and information regarding an individual is stored securely and is never left on desks or in filing trays unless in a locked office that has limited access.
- If a combination of electronic and paper based data is being stored regarding an individual, information should be cross referenced to make a complete file to ensure that two separate differing records are not being kept.

3.8 Carrying Data outwith Offices

There may be times, where staff and volunteers are required to carry personal data outwith their office base. This information should be kept to a minimum and should be carried electronically wherever possible. Hard copy information should only be carried if there is no other option. In these cases the following should apply in relation to hard copy information:

- Information should only be taken out of the office if there is a clear purpose for the information.
- The data and information should be anonymised as far as possible to protect the identity of the individual.
- The information should be stored in a secure bag.
- All team members should be aware of their responsibilities relating to the security of the data and information they are carrying.

In relation to electronic information stored on USB stick or laptop/netbook, the following should apply:

- As above the information should be necessary and relevant and limited as far as possible.
- As above the information should be anonymised as far as possible.
- Any mobile devices should be encrypted and password protected. Team members

should be aware that is their responsibility to keep that data and information safe and secure They must take all reasonable precautions to ensure that information is not lost or stolen.

4. Retention and Archiving

4.1 Retention Timescales

It is essential that we do not keep data and information that we are not required to keep. As this is the case, we have a retention schedule in place which should be followed by all team members and data and information should not be kept beyond these timescales, this can be found in Appendix 1 of our Privacy Policy GCS 2.16.

When archiving data and information, both paper based and electronic, detailed on the box or file should be the date when the information will be destroyed in line with the retention timelines.

Retention timescales also apply to information that is held on databases.

4.2 Retention of General Office Files

Whilst there is no specific legislation in connection with general office files such as general correspondence, minutes of internal meetings etc, Osprey Housing Group recommends that general files should kept in the office for one year and thereafter should be archived for no longer than 2 years. Unless a record of signatures is required, the majority of general office information should be held electronically rather than by hard copy. This will avoid any unnecessary storage.

As per section 12, CCTV records should be kept for no longer that 7 days unless the recording is being used in an investigation. Where this is the case it is suggested that recordings are held for no longer than four years. The timescales will also ensure that data and information is manageable and can be stored and accessed effectively.

4.3 Considerations when Deciding on Retention Periods

Osprey Housing Group staff should consider the following questions when deciding how long to retain a record before final disposition:

- Is the record still required for the day-to-day running of the association?
- Is it required for legal purposes (e.g. contracts)?
- Does any legislation or official regulation govern how long it must be kept?
- Is it likely to be of ongoing or recurrent public interest?

Retaining Records for Permanent Preservation Records are designated as "archival" for many reasons, the main ones being that:

- they are still essential to the governance of Osprey.
- they document Osprey's policies, structures and processes so that its activities may be accountable to the present generation and understood by future generations.

In general, this means keeping records which provide evidence of the following matters:

- top-level decision making and policy formulation within Osprey.
- policy making within the major functions of Osprey.
- important or high profile aspects of the interactions between Osprey and individuals, businesses, civic institutions, and the environment.
- principal administrative processes of the organisation structure and remit of the organisation, and any major changes to these.

4.4 Archiving Guidance and Procedures

As per section 3.7, Storage of Information, only current data and information that is in use should be kept in office files. This would usually be information relating to that calendar year or financial year for financial paperwork. Where possible these types of documents should be scanned as soon as possible. All other information should be electronically archived.

Where possible data and information should be archived electronically in order to save space and in some case to save money where external storage would be required. All departments should review the data and information they hold on a regular basis.

When archiving information team members should include the following:

- Any information that is over a year old should be electronically archived as per the retention schedule.
- Any information that is not required should be destroyed as per the retention schedule.
- Any information that is archived and due to be destroyed as per the retention schedule.

When archiving data and information, electronically or in hard copy, the following should be applied:

- The data and information should be stored in a tidy and logical system.
- The archive box or electronic file should be labelled with the following information:
    - What is the data and information is e.g. Invoices,
    - The date that relates to the information e.g. September to November 2010
    - When the data and information should be destroyed
    - File/box number

All archived material should be boxed and marked up appropriately (as above) and given to the Corporate Services team for delivery to the archive in Lossiemouth.

4.5 Disposal Arrangements

It is essential that the disposal of records is undertaken in accordance with these policies and procedures. All paper based records containing personal information should be shredded or disposed of through confidential waste systems. All electronic records containing personal information should be deleted completely from the hard drive.

Records which are not selected for permanent preservation and which have reached the end of their administrative shelf life should be destroyed in as secure a manner as is necessary for the level of confidentiality or security markings they bear.

4.6 CCTV Systems

CCTV and other systems which capture images of identifiable individuals are also covered by legislation. Before deciding to install or to continue using a CCTV system it is important to conduct an impact assessment to determine if CCTV is justified and how it should be operated. Issues to consider in the impact assessment include:

- Who will be using the CCTV images? Who will take legal responsibility?
- What is the purpose for using CCTV? What problems will it address?
- What benefits are to be gained from its use?
- Are images of identifiable individuals required?
- Will the system remain suitable in the future?
- What future demands may arise for wider use of images and how will these be addressed?
- What are the views of those who will be under surveillance?
- What can be done to minimise intrusion for those who will be monitored? It is essential that appropriate camera equipment and locations are selected.

Image capture should be restricted to ensure that cameras do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property. Cameras must be sited and the system must have the necessary technical specification to ensure that images are of the appropriate quality.

A regular maintenance regime must be set up to ensure that the system continues to produce high quality images. Regular checks must be carried out to ensure that the date and time stamp recorded on the images is accurate.

Recorded material must be stored securely and in a way that prevents damage to the image. Recorded images should be viewed in a restricted area, such as a designated secure office. Disclosure of images from the CCTV system should be controlled. Consideration should be given as to whether a request for disclosure is genuine and if there is any risk to other people involved.

Images should not be kept for longer than is necessary. The timeframe for keeping images will be set on our equipment. On occasion it may be necessary to keep images

for a longer period, for example where they are being used by a law enforcement body investigating a crime. It is suggested that such footage is held for four years.

CCTV signs must be displayed in order to let people know that they are in an area where CCTV surveillance is being carried out. A CCTV code of practice is available from the Information Commissioner's Office website: www.ico.gov.uk

7. Equal Opportunities

The Group shall strive to ensure equality of opportunity, and by definition, that all individuals are treated fairly regardless of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation. The Group opposes, and shall adopt a zero tolerance stance towards, all forms of unlawful discrimination, harassment and victimisation.

In this regard, the Group acknowledges the protected characteristics and types of unlawful behaviour defined within the Equality Act 2010. As a minimum all practices shall aim to ensure compliance with the legislative provisions therein.

8. Monitoring & Reporting

We will monitor this policy in conjunction with our other policies and procedures to ensure that it is being adhered to.

9. Review

This policy will be reviewed every 3 years unless the following criteria dictate that it would be best practise to review sooner:

i. applicable legislation, rules, regulations and guidance, both those which affect the Group directly and those which affect the resources available to significant numbers of our customers to enable them to sustain tenancies.
ii. changes in the organisation.
iii. continued best practice.

Appendix 1
A Quick 'How to Comply' Checklist

This short checklist will help comply with the legislation. Being able to answer 'yes' to every question does not guarantee compliance, but it should mean that you are heading in the right direction. If you are unsure talk to your Line Manager and/or the Corporate Services Manager.

- Do I really need this information about an individual?
- Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- Am I satisfied the information is being held securely, whether it's on paper or on computer?
- What about our website? Is it secure?
- Am I sure the personal information is accurate and up to date?
- Do I delete/destroy personal information as soon as I have no more need for it?
- Is access to personal information limited only to those with a strict need to know?
- If I want to put staff details on our website have I consulted with them about this?
- If I use CCTV, is it covered by the Act? If so, am I displaying notices telling people why I have CCTV? Are the cameras in the right place, or do they intrude on anyone's privacy?
- If I want to monitor staff, for example by checking their use of email, have I told them about this and explained why?
- Have I trained my staff in their duties and responsibilities under the Act, and are they putting them into practice?
- If asked to pass on personal information, am I and my staff clear when the Act allows me to do so?
- Would I know what to do if one of my employees or individual customers asks for a copy of information I hold about them?
- Have I checked with our Privacy Policy GCS 2.16, the Osprey policy for dealing with data protection issues?
- Do I need to notify the Information Commissioner? If I have already notified, is my notification up to date, or does it need removing or amending?