Data Protection Policy and Procedure

AS WITH ALL OF THE ASSOCIATION'S POLICIES and PROCEDURES, THIS GUIDE, IN FULL AND IN PART, CAN BE MADE AVAILABLE IN SUMMARY, ON TAPE, IN BRAILLE, AND IN TRANSLATION INTO MOST OTHER LANGUAGES –

PLEASE ASK A MEMBER OF STAFF IF YOU WOULD LIKE A VERSION IN A DIFFERENT FORMAT

New Version Approved By	Committee at the meeting on 6th February 2019
Last Reviewed (partial)	June 2019
Next Review	February 2022

1. Introduction and General Information

1.1. During the course of Whiteinch & Scotstoun's (WSHA's), WS Property Management's (WSPM) and WS Estate Services (WSES's) activities the organisations will process Personal Data (which may be held on paper, electronically, or otherwise) about staff, Committee/Board Members and customers and they recognise the need to treat it in an appropriate and lawful manner, in accordance with the Data Protection Legislation. For the purposes of simplicity, hereafter the three organisations will be treated as if under the blanket of WSHA as 'the Association'. The purpose of this policy is to make staff, Committee/Board Members and customers aware of how the Association handles Personal Data and what the Association expects in return to ensure WSHA complies with the legal requirements.

1.2. The Association, and its subsidiary companies, are individually registered with the Information Commissioner as Data Controllers under the Data Protection Legislation and take all reasonable steps to ensure that practices in the handling of personal information are of a high standard and comply with this Legislation. This includes, for example, using self-assessment and internal audit to help flag up areas requiring attention.

1.3. The Data Protection Policy and Procedure is intended for use by Association Staff for instance:

- when they are faced with a request to disclose information, whether this be a tenant ringing up to enquire about their own rent account or a request for information on a tenancy matter from a third party, such as the DSS, or

- when they require guidance on what information should be retained (and for how long) once it is no longer relevant to the Association carrying out its day-to-day business.

1.4. In drafting the procedure, the Association has tried to cover the vast majority of ways in which information is likely to be requested or retained. Exceptionally, however, the procedure may be silent on how to deal with any query that is made. In such circumstances, the Chief Executive/Deputy Chief Executive (or another member of the Executive Team if (s)he is not available) will decide on whether the disclosure is to be made/information is to be retained – with appropriate legal advice in cases where this is considered advisable.

1.5. This policy does not form part of any employee's contract of employment and the Association may amend it at any time.

2. Equal Opportunities

2.1. In relation to data protection, this means that the Association is committed to ensuring that no tenant is unable to, or discouraged from, understanding and exercising their rights under the data protection legislation because they sometimes find it difficult to

fully understand documents produced in regular printed English.
This means that the Association will provide documents upon request:

- in large print or on coloured paper for those with visual impairment or deteriorating eyesight
- on tape for those who are unable to read printed matter
- in Braille for those who prefer this means of communication
- translated into another language, or, if this is impractical, access to a translating service
- in any other feasible format that tenants may find helpful.

2.2. The Association is also happy to discuss any request to provide copies of the information held in an alternative format.

3. Definitions

3.1. **"Compliance audit"** means the record of how the Association meets the requirements of the Data Protection Legislation.

3.2. **"Consent"** means any freely given, specific, informed and an unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to him or her.

3.3. **"Data Subject"** means an identified or identifiable natural person

3.4. **"Data Protection** Legislation**"** means

- the Data Protection Act 2018 (DPA 2018), (and in relation to any of its provisions which are not yet in force; from the date(s) upon which such provisions come into force) and any regulations and secondary legislation implementing or in relation to the DPA 2018;
- the General Data Protection Regulation ((EU) 2016/679) (GDPR) and any national implementing laws, regulations and secondary legislation, for so long as the GDPR is effective in the UK; and
- any other replacement or supplementary legislation relating to the Processing of Personal Data (for example in relation to any exit by the UK from the European Union).

3.5. **"EEA"** means the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

3.6. **"Personal Data"** means any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable natural person is one who can be identified,

directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person.

3.7. **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise Processed.

3.8. **"Process" and "Processing"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.9. **"Pseudonymised"** means Processing Personal Data in such a manner that the Personal Data can no longer be attributed to an individual without the use of additional information which is meant to be kept separately and secure.

3.10. **"Special Categories of Personal Data"** means Personal Data revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

3.11. **"Supervisory Authority"** means an independent public authority which is established by a Member State, for the UK our Supervisory Authority is the Information Commissioner's Office ("**ICO**").

4. General Principles of Data Protection

4.1. When Processing data the Association will comply with the Data Protection principles set out in the Data Protection Legislation, which say that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner;
- collected only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed;
- accurate and where necessary kept up to date;
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed;
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage;

- not transferred to another country without appropriate safeguards being in place; and

- made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data.

5. Your rights

5.1. Personal Data shall be Processed in a fair, lawful and transparent manner

- The Association will usually only Process Personal Data where it has a legal basis for Processing; namely that the Processing is for its legitimate interest or the legitimate interest of others; it is necessary for the performance of the contract or where the Processing is necessary to comply with legal obligations. In other cases, Processing may be necessary for the protection of the person's vital interests or the Association has obtained Consent. Further details are set out in the Association's Privacy Policy displayed on the home page of its website or its Employee Privacy Statement.

- The Association will only process "Special Categories of Personal Data" where a further condition is also met. Usually this will mean that the Data Subject has given their explicit Consent, or that the Processing is legally required for employment purposes.

5.2. **Processing for limited purposes**

The Association will only process Personal Data for the specific, explicit and legitimate purposes or purposes set out in clause 5.1 above. Personal Data will not be further processed in any manner incompatible with those purposes unless the Association informs the subject of the new purpose(s) and obtained consent where necessary.

5.3. **Processing shall be Adequate, relevant and limited to what is necessary**

The Association does not collect any Personal Data beyond what is necessary and will collect only such Personal Data as is required. The Association will ensure that the Personal Data collected is adequate and relevant for the intended purpose.

5.4. **Personal Data shall be Accurate and up to date**

The Association will endeavour to keep the Personal Data the Association stores accurate, complete, up to date and relevant to the purpose for which the Association collected it. Where the Association becomes aware that Personal Data is inaccurate or out of date the Association will correct or delete the relevant record without delay.

It is the obligation of staff, Committee/Board Members and customers to notify the Association if their personal details change or if they become aware of any inaccuracies in the Personal Data the Association holds.

5.5. Data retention and storage

5.5.1. The Association will not keep Data Subjects' Personal Data for longer than is necessary for the legitimate business purpose or purposes for which the Association originally collected it and where appropriate, for the purposes of satisfying any legal, accounting, or reporting requirements. This means that Personal Data will be destroyed [or erased from our systems] when it is no longer required in accordance with our Data Retention Schedule including requiring third parties to delete such data where applicable. Please contact the Deputy Chief Executive for further information of the Association's policies and procedures in relation to the retention of your Personal Data.

5.5.2. The Association has mapped the data that it processes on each Data Subject Category including the type of data, the purpose for collection, who the data is shared with and the retention periods. Please contact the Deputy Chief Executive if you would like further information. If you find in your role that you are required to collect new Personal Data please contact the member of the Executive Team responsible for your role so that the data mapping can be updated and the Association can confirm the legitimate reason for collection].

5.5.3. The Data Retention Schedule explains the Association's requirements for staff with regards to how they retain retention, storage and disposal of personal data, and to dispose of personal data and provides guidance on appropriate data handling and disposal of personal data.

5.5.4. Failure to comply with this Policy will expose the Association to the risk of threat to its security and to potential legal and/or regulatory action, leading to investigation, censure, judicial claims, fines and penalties; to adverse publicity, damage to its reputation, loss of revenue; or to difficulties in providing evidence when we need it and in general running of our operation. Due to the potential severity of the consequences, any breach of this Policy may be considered a matter for disciplinary action.

5.5.5. Personal information is stored securely. Where this is in paper files, these are placed in lockable cabinets when not in use; computer files are password protected and e-mails encrypted. To ensure cybersecurity all Staff are required to follow the Guidance on Email & Internet Access which is an appendix to the Information & Cybersecurity Policy and any breach of the Guidance may be considered a matter for disciplinary action.

5.5.6. It is unavoidable that, from time to time, files and other information may have to be removed from the Association's office, for example, to carry out a house visit.

5.5.7. Staff are required to take the utmost care not to misplace or lose any information. In the event that this does occur, however, the Deputy Chief Executive should be notified at the earliest opportunity.

5.6. **Processing shall be in line with the rights of any Data Subject**

The Data Subject has the right to:

5.6.1. a) notify the Association that he/she wishes to withdraw his/her Consent (where his/her Consent is the legal basis for Processing) to processing at any time;

5.6.2. request certain information about the Association's Processing of his/her Personal Data;

5.6.3. request access to any Personal Data the Association hold about him/her;

5.6.4. ask the Association to erase his/her Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate or incomplete Personal Data;

5.6.5. ask that Processing is restricted in specific circumstances;

5.6.6. prevent Processing that is likely to cause unwarranted substantial damage or distress to him/her or anyone else;

5.6.7. challenge Processing which has been justified on the basis of the Association's legitimate interests, or in the public interests;

5.6.8. be notified of a Personal Data breach which is likely to result in high risk to his/her rights and freedoms;

5.6.9. make a complaint to the ICO;

5.6.10. in limited circumstances, receive or ask for his/her Personal Data to be transferred to a third party in a structured, commonly used and machine readable format; and

6. <u>What Does the Data Protection Legislation Mean for The Association on a Day-to-Day Basis?</u>

6.1. **Security**

6.1.1. The Association implements and maintains all reasonable and appropriate technical and organisational measures to prevent Personal Data Breaches. Particular care is taken in protecting Special Categories of Personal Data.

6.1.2. The Association has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. The Association will only transfer Personal Data to a third party if the third party enters into an agreement with us to ensure that they will comply with obligations which are at least as strict as the terms of this Policy, to allow us to maintain the protection of your Personal Data, and who agree to put adequate measures in place, as requested.

6.1.3. Maintaining data security under clause 6.1.2 means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the Personal Data.

6.2. Sharing Personal Data with third parties

6.2.1. The Association may have to share Data Subjects' data with third parties, including third-party service providers and other entities in the Association's group. The Association require third parties to respect the security of the Personal Data and to treat it in accordance with the law.

6.2.2. The Association will share Personal Data with third parties where required by law, where it is necessary to administer the working relationship, in circumstances where it is in staff, Committee/Board Members' or customers' interests, or where the Association has another legitimate interest in doing so.

6.2.3. With regard to other Data Subject Personal Data staff should refer to the Privacy Policy found on the Association's website which identifies which data can be shared with other third parties and the lawful grounds for doing so. For instance:

- if required by law or by any regulation which governs us, the Association will share information with third parties – these might include governmental or quasigovernmental organisations, law enforcement authorities, courts and arbitrators from time to time;

- the Association will share information when absolutely necessary for management of the property the Data Subject occupies;

- the Association will share information with other councils, where appropriate – for example, if the Data Subject moves between council catchments; and

- the Association may share information with certain Third Party Service Providers. These include contractors and designated agents and other entities within the Association's group. For example, the following activities are carried out by Third Party Service Providers: IT Services, Legal Services and Community Safety Services.

6.2.4. There may be other instances, when the Association obtains Consent from the Data Subject.

6.2.5. Staff do, regularly have to disclose information about someone to:

- the person themselves
- their legal appointee
- someone acting on their behalf

The critical point for staff for disclosure is therefore whether they are satisfied that the person asking for the information is being truthful about their identity and, where the enquirer is not the tenant, that they have a right to be told the information.

The Association will therefore adopt the "key question" approach already used by many companies in the UK. This involves the tenant or data subject having to respond correctly to a unique question that they would definitely know the answer to, for example, what is your date of birth?

Where the enquirer is not the tenant, but a representative, staff must ensure that there is a signed mandate on file before disclosing any information.

6.3 As experience of this policy is gained, an additional guidance document will be developed. Meantime, where there is any uncertainty, referral should be made to the Chief Executive/Deputy Chief Executive (or another member of the Executive Team if (s) he is not available).

7. Data Subject Request

7.1. Any Data Subject, such as one of our tenants, has the right to request access to the Personal Data the Association holds, including the right to request confirmation that the Association processes the Data Subject's Personal Data, receive certain information about the processing of the Personal Data, and obtain a copy of the Personal Data the Association processes.

7.2. For further information about the process you should follow to access your personal data please refer to the Subject Access Procedure: Employees. With regard to the process you should follow about other Data Subjects please refer and adhere to the Subject Access Procedure: Non-Employees.

8. Personal Data Breaches

8.1. The Association has put in place procedures to deal promptly and effectively with any suspected Personal Data Breach and will notify the Data Subject and/or the Information Commissioner's Office (ICO) where the Association are legally required to do so. The Scottish Housing Regulator will also be advised as an ICO notification has been confirmed as a Notifiable Event.

8.2. If a Data Subject considers that this policy has not been followed in respect of his/her Personal Data he/she should raise the matter immediately with the Deputy Chief Executive.

8.3. In addition, all employees, workers, Committee Members and contractors should alert the Deputy Chief Executive immediately if they discover or suspect a data breach however small. This allows the Association to consider any measures to reduce the immediate impact and, comply with its legal and regulatory duties which include the requirement to notify the ICO within 72 hours.

8.4. The Association expects all its employees, workers, Committee Members and contractors to adhere to the Personal Data Breach Procedure. Adherence to the Procedure is mandatory and non-compliance could lead to disciplinary action.

9. Other relevant key Policies & Procedures

9.1. This policy compliments the Association's confidentiality policy. Only information which can or must be lawfully disclosed under the Data Protection Legislation will be shared with a third party without the individual's consent.

9.2. The Subject Access Request Procedure provides details of how the Association will respond when a data subject exercises their rights in relation to their personal data.

9.3. The Data Breach Procedure provides further details of the process to be followed in the event of a potential personal data breach.

9.4. The Mobile Phone Procedure provides guidance on keeping data safe on mobile phones.

9.5. The Email & Internet Procedure provides guidance on Cybersecurity.

9.6 On occasions when the Committee of Management has to consider items of a confidential nature, these will generally be presented as paper copies to be distributed at the Meeting in question. At the close of the Meeting, all copies will be collected and disposed of by the senior staff members in attendance using the Association's confidential shredding system.

9.7 Should the paperwork involved be too extensive to allow adequate consideration to be afforded on a first viewing, paper copies will be delivered to Members with a reminder of the sensitivities involved and the expectation that they should be returned at the Meeting for disposal, as above. If a Member cannot attend a Meeting, they should advise before delivery, if known, or otherwise arrange for collection or personal return to the Office.

10. Responsibilities for Compliance

10.1. The Deputy Chief Executive has overall responsibility for data protection within the Association, and for ensuring that the Association's notification to the Information Commissioner's Office, and all entries in the Data Protection Register, is accurate and up to date. This will be checked at least every two years, or in the intervening period if this officer considers that this needs to be changed (because, for example, the Association has broadened the way it operates).
A checklist is provided as Appendix 1.

10.2. Members of the Executive Team will assist in implementing the requirements of the Data Protection Legislation by:

- providing advice and support to all departments on all matters relating to compliance with the Data Protection Legislation
- disseminating information relating to the Data Protection Legislation
- responding to requests from individuals to access personal information the Association holds about them
- maintaining the internal Data Protection Log which contains details of all requests for access to information under the terms of the Data Protection Legislation

10.3. The Deputy Chief Executive has specific responsibility for Personal Data held on employees. Staff will be informed about data protection issues, and their rights to access their own personal data through the staff handbook and induction courses.

10.4. Departmental managers will ensure that personal data processed by their department included in the Association's Data Protection Register entry is kept up to date, and complies with the principles and rights.

10.5. All staff have a responsibility to fully comply with the requirements of the Data Protection Legislation and this procedure. When involved in requesting information, staff will explain why the information is necessary, what it is to be used for, and who will have access to it.

10.6. The Association and all staff who use any personal information must ensure that they follow the above principles and rights at all times. In-house training will therefore be provided on these principles and the Association's procedures for all relevant staff and new staff will have this incorporated into their induction process.

10.7. The Association is responsible for and must be able to demonstrate compliance with the principles and rights listed above.

11. Role of Internal Audit in Data Protection

11.1. Failure to observe practices that help the Association comply with the Data Protection Legislation could expose the organisation to a certain degree of risk. Keeping this policy and procedure up to date and ensuring that staff are aware of its contents is one way of helping guard against any legal breaches. As an added safeguard, the internal auditor will be required to comment on data protection at least once in every three years.

11.2. The Data Protection Officer and Depute Chief Executive will review any changes and updates to the Compliance Audit on an annual basis.

11.3. The Management Committee will receive an annual report on the number of Subject Access Requests and Personal Data Breaches. They will also be notified as soon as reasonably practicable of the details of any Personal Data Breach.

12. Equal Opportunities Testing

12.1. In accordance with the Association's Equality & Diversity Policy, this Policy has been consciously considered to judge whether there is any likelihood that its presentation or operation could in any way lead, no matter how inadvertently, to discrimination. The conclusion of this exercise is that it is believed that the Policy should operate in a non-discriminatory way.

13. Policy Review and Changes

13.1. The Policy will be reviewed initially after three years, the five thereafter, or sooner in line with changes in legislation or best practice.

APPENDIX 1

Data Protection Checklist

This checklist is intended to be completed on a self-assessment basis to help the Association identify possible areas for action. An assessment will be carried out by the Deputy Chief Executive every two years and a report prepared for the Management Committee.

An explanation of each response should be provided in Section 1 and any required follow-up action, together with timescales noted in Section 2.

Section 1 – Current Position

Question		Response (with explanation)
1.	Is there a written policy covering data protection issues?	Yes ☐ No ☐ N/A ☐
2.	Is there a contact person for data protection?	Yes ☐ No ☐ N/A ☐
3.	Are there fair obtaining/opt in boxes on your literature/forms?	Yes ☐ No ☐ N/A ☐
4.	Is there a procedure for responding to requests for information, and a log of who it is disclosed to?	Yes ☐ No ☐ N/A ☐

Question		Response (with explanation)
5.	Are comments by staff in data records professionally expressed? – would they survive a subject access request?	Yes ☐ No ☐ N/A ☐
6.	Are access controls clear and robust?	Yes ☐ No ☐ N/A ☐
7.	Do disclosure procedures accept the possibility of third parties trying to obtain data by deception? Do staff know how to handle such requests?	Yes ☐ No ☐ N/A ☐
8.	Are your Data Protection registrations up to date and accurate?	Yes ☐ No ☐ N/A ☐
9.	Have staff and the Board undertaken Data Protection awareness training?	Yes ☐ No ☐ N/A ☐
10.	Do you review access rights of employees leaving the organisation to ensure data cannot be removed or passed to a third party?	Yes ☐ No ☐ N/A ☐

Question		Response (with explanation)
11.	Has data protection audit been included in the internal audit programme?	Yes ☐ No ☐ N/A ☐
12.	Do you have a written contract with any third party who can access personal information, about their information processing and security?	Yes ☐ No ☐ N/A ☐

Assessing Officer: _____

Date: _____