Data Protection Policy

Responsible Officer:	Director of Legal & Governance
Approved:	May 2018
Review Date:	May 2020
Version:	1
Scope:	Group Wide

Contents:

Introduction

Incommunities uses information as a tool as part of its business. We comply with out legal and regulatory obligations under the General Data Protection Regulations and the Data Protection Act 1998. In addition, we seek to use information effectively in order to meet our objectives under our corporate strategy.

The Data Protection Policy incorporates procedural steps to take in given situations. It is designed to be a practical document that employees will be able to use to solve problems as they arise. Advice and assistance can be obtained from the Data Protection Helpdesk, which can be contacted at:

DataProtection.Helpdesk@incommunities.co.uk

1.0 Legal Framework

1.1 The Data Protection Principles

Incommunities abides by the Data Protection Principles in relation to the processing of personal data, which are:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality (security)
- accountability

The Data Protection Principles are at the heart of everything we do in relation to processing personal data.

1.2 Privacy Notice

Incommunities uses Privacy Notices to provide information to people whose personal data is being processed. The Privacy Notice provides the information in a concise, transparent, intelligible, easily accessible form using clear and plain language. Different Privacy Notices will be used, as appropriate, to provide information to people whose personal data is being processed e.g. a wider Privacy Notice for tenants and similar, a more focussed Privacy Notice for job applicants, employees and former employees.

1.3 Lawful processing of personal data

The primary justifications for processing personal data that Incommunities use are as follows:

- the processing is necessary for the performance of, or entering into, a contract with the person whose data is being processed e.g. a Tenancy Agreement, employment contract.

- the processing is necessary for the purposes of the legitimate interests pursued by the Incommunities or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the person whose data is being processed which require protection of personal data, in particular where the data subject is a child. For example, Incommunities has a legitimate interest in tackling anti-social behaviour affecting our tenants, therefore the processing of a non-resident's name and evidence of their ASB is justified because the perpetrator cannot except their privacy to outweigh our legitimate interest.

- the processing is necessary for Incommunities to comply with our legal obligations e.g. making a safeguarding referral, undertaking a health and safety risk assessment.

- the person whose personal data is being processed has given consent e.g. an applicant for housing consents to Incommunities using their information to identify and offer suitable housing.

- on a rarer basis, Incommunities justifies the processing of personal data because the processing is necessary to protect someone's vital interests (e.g. a member of staff may provide paramedics with known illnesses of a person in an emergency) or the processing is necessary to exercise official authority invested in Incommunities (e.g. the issuing of Community Protection Notices).

1.4 Using consent to justify the processing of personal data

Generally, Incommunities justifies the processing of personal data without relying on the consent of the person whose data is being processed. Where consent is one of the justifications, or the sole justification, Incommunities must be able to evidence that explicit consent has been given, preferably in writing, and that it was given freely following a request that was capable of being understood. Consent can be withdrawn, in which case any further processing of personal data should either cease (which may result in the cessation of the provision of services to the person whose personal data was being processed) or it can continue if at least one other justification exists.

1.5 Processing special categories of personal data

Incommunities processes the following special categories of personal data with the following typical justifications:

Special category of personal data	Justification	Example
Racial or ethnic origin	Employment law obligations. Occupational health. Explicit consent. Public knowledge brought about by the person whose personal data it is. Legal disputes.	Incommunities monitors racial or ethnic origin for equality and diversity purposes.

Religious or philosophical beliefs	Employment law obligations. Explicit consent. Public knowledge brought about by the person whose personal data it is. Legal disputes.	Incommunities monitors religious or philosophical beliefs for equality and diversity purposes.
Trade union membership	Employment law obligations. Explicit consent. Public knowledge brought about by the person whose personal data it is. Legal disputes.	Incommunities deducts trade union subscriptions on behalf of employees upon request.
Health	Employment law obligations. Occupational health. Explicit consent. Public knowledge brought about by the person whose personal data it is. Legal disputes. Vital interests.	Incommunities handles health personal data when managing sick leave.
Sex life	Substantial public interest. Explicit consent.	Incommunities would be under a duty to make a safeguarding referral if a person's sexual activity endangered a child or vulnerable adult.
Sexual orientation	Employment law obligations. Explicit consent. Public knowledge brought about by the person whose personal data it is. Legal disputes.	Incommunities monitors sexual orientation for equality and diversity purposes.
Criminal convictions and offences (not a special category in law)	Statutory rights.	Incommunities processes alleged and proven criminality when tackling anti-social behaviour.

1.6 Lawful processing of anonymised data

Where personal data has been anonymised, Incommunities may use the anonymised data. The person whose data it was (before anonymization) cannot exercise their rights to access, rectification, erasure, restriction of processing, or portability in relation to the anonymised data. Any such request should be referred to the Data Protection Officer as soon as possible.

2.0 Incommunities'/Sadeh Lok's Responsibilities and the Responsibilities of Joint Controllers and Processors

2.1 Incommunities/Sadeh Lok Responsibilities

Incommunities/Sadeh Lok recognises its responsibilities as a data controller. Incommunities/Sadeh Lok will implement appropriate technical and organisational measures to comply with data protection laws. Incommunities/Sadeh Lok processes significant amounts of personal data as a housing provider, employer, head contractor, sub-contractor, and partner to other agencies. The risks relating to personal data, privacy and information governance are recognised and managed appropriately through the Risk Register, the Assurance Process and by being overseen by the Audit & Risk Committee.

Key Performance Indicators such as the number of data breaches (with some narrative) and the number of requests for personal data received, including confirmation that they were resolved within the deadline, are reported to the Common Board annually. Major data protection projects, such as the implementation of the GDPR, are reported more regularly and in more detail to the Board and Committees within the governance structure.

2.2 Joint controllers' responsibilities

Incommunities/Sadeh Lok is a joint controller of data with other organisations in some circumstances. This includes many of our contracts where both (or all) parties to the contract decide the purpose and method of processing the personal data involved. It also includes partnering relationships such as Incommunities/Sadeh Lok and West Yorkshire Police, where both parties decide the purpose and method of processing the personal data involved.

Where there are joint controllers, the respective responsibilities of each party to comply with data protection laws (in particular in relation to individuals exercising their data protection rights, and the provision of Privacy Notices) will be determined transparently. This will often be achieved through a contract or an Information Sharing Agreement.

The essence of the arrangement between joint controllers will be made available to the individuals whose personal data is being processed. This will be achieved through the Privacy Notices of the joint controllers.

2.3 Processors' responsibilities

Incommunities/Sadeh Lok uses other organisations or individuals to process the personal data we hold, in order to meet our business needs. Processors are expected to:

- provide sufficient guarantees to implement appropriate technical and organisation measures to comply with data protection laws (e.g. provide copies of satisfactory data protection policies and procedures)
- not use another processor unless Incommunities/Sadeh Lok's has given express permission and, if so, ensure that the other processor is subject to the same data protection compliance obligations as the processor is

- abide by the terms and conditions of the contract or agreement
- process personal data as per Incommunities/Sadeh Lok's instructions
- ensure that their employees and contractors are legally bound by a duty of confidentiality
- implement appropriate technical and organisational measures to maintain adequate security relating to the processing
- assist Incommunities/Sadeh Lok in meeting our data protection obligations
- delete or return all personal data to Incommunities/Sadeh Lok after the processing, as per Incommunities/Sadeh Lok's instructions, unless legal obligations require the processor to store it
- comply with data protection audits, inspections and similar undertaken by Incommunities/Sadeh Lok or our agent
- supply copies of any approved code of conduct and/or certification that the processor relies upon to demonstrate their compliance with data protection laws e.g. ISO27001.

It is the responsibility of Incommunities/Sadeh Lok's staff managing contracts or agreements with processors to uphold the above expectations.

3.0 The Consequences of Breaching Data Protection Obligations for /Sadeh Lok, their Staff and their Contractors

3.1 Consequences for Incommunities/Sadeh Lok

Incommunities/Sadeh Lok understands that breaching data protection obligations will have consequences. These may include:

- a complaint being made against Incommunities/Sadeh Lok to the Information Commissioner or via our internal complaints process, which may require resources to be spent dealing with the complaint and may cause reputational harm
- legal action being taken against Incommunities/Sadeh Lok by a third party for breach of data protection laws, which may lead to compensation being awarded
- imposition of an administrative fine by the Information Commissioner for breach of data protection laws, which can be up to 20M Euros
- receiving a warning, reprimand or order from the Information Commissioner; Breach of contract proceedings or action by third parties.

3.2 Consequences for staff

Staff who are responsible for a breach of data protection laws may be subject to disciplinary and/or capability proceedings. Please see the Code of Conduct, the ICT Code of Conduct and relevant HR policies and procedures for more detail.

3.3 Consequences for contractors

Third parties that contract with Incommunities/Sadeh Lok may, if they have breached data protection laws (whether relating to their contract with Incommunities/Sadeh Lok or otherwise) or Incommunities/Sadeh Lok policies or instructions, face legal action being taken and/or the termination of their contract. They may also be added to the 'no contract' list (please see the separate policy relating to this).

3.4 Procedure upon becoming aware of possible consequences of a data protection breach

Any member of staff, and any contractor, who becomes aware of any of the possible consequences listed above (e.g. receives a complaint from an individual about breaching data protection or receives a letter from the Information Commissioner) must inform the Data Protection Helpdesk as soon as reasonably practicable. The Data Protection Officer will then handle the matter, or delegate the matter as appropriate.

4.0 Data Protection Officer (DPO)

4.1 A Data Protection Officer (DPO) shall be appointed by Incommunities Group Ltd. The appointee will be the DPO for Incommunities Group Ltd and all of its wholly-owned subsidiaries. The DPO will be required to possess qualifications and/or experience that make them suitable to fulfil the DPO's tasks.

The Group companies, and their employees, will ensure that the DPO is involved in data protection issues properly and in a timely manner. This includes the Group companies providing adequate resources to the DPO, allowing the DPO access to personal data and processing operations, and maintaining the DPO's knowledge and skills.

The DPO is not subject to instruction on data protection matters, and will not be dismissed or penalised for performing DPO tasks undertaken competently and in good faith. The DPO will report to the Executive Management Team.

4.2 The DPO will undertake the following tasks, amongst other things:

- Advising the Group companies and their employees of their data protection obligations;
- Monitoring compliance with data protection obligations and the Data Protection Policy;
- Advising on Data Protection Impact Assessments, upon request;
- Co-operating with the Information Commissioner;
- Investigating data protection breaches and, as appropriate, reporting them to the Information Commissioner;
- Reporting annually to the Common Board on data protection matters.

4.3 The contact details of the DPO will be published on the company websites. The Information Commissioner will be notified of the DPO's contact details. The DPO will delegate some tasks to appropriately trained staff and/or external contractors. The staff/contractors will undertake tasks as delegated, including completing data protection tasks in the DPO's absence.

5.0 Data Protection by Design & Data Protection Impact Assessments

5.1 Data Protection by Design

Data Protection by Design, sometimes known as Privacy by Design, is an approach to projects that promotes privacy and data protection compliance from the start. It requires Incommunities/Sadeh Lok to implement appropriate technical and organisational measures to meet the Data Protection Principles. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- potential problems are identified at an early stage, when addressing them will often be simpler and less costly
- increased awareness of privacy and data protection across an organisation
- organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act
- actions are less likely to be privacy intrusive and have a negative impact on individuals.

The seven internationally-recognised principles of Data Protection by Design are:

1. Proactive and preventative, not reactive and remedial

Data Protection by Design seeks to anticipate and remedy problems rather than problems occurring and having to be dealt with

2. Privacy as the default setting

Data Protection by Design seeks to deliver the maximum degreeof privacy by ensuring that personal data are automatically protected in any given IT system or business practice

3. Privacy Embedded into Design

Data Protection by Design is embedded into the design and architecture of IT systems and business practices.

4. Full Functionality — Positive-Sum, not Zero-Sum

Data Protection by Design seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner.

5. End-to-End Security — Full Lifecycle Protection

Data Protection by Design extends securely throughout the entire lifecycle of the data involved. Strong security measures are essential to privacy, from start to finish.

6. Visibility and Transparency — Keep it Open

Data Protection by Design seeks to assure all stakeholders that whatever the business practice or technology involved, operating according to the stated promises and objectives, subject to independent verification.

7. Respect for User Privacy — Keep it User-Centric

Data Protection by Design requires measures such as strong privacy defaults, appropriate notice, and empowering user-friendly options.

5.2 Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs) help us to identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. They are a tool that we use. You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals
- large scale processing of special categories of data or personal data relation to criminal convictions or offences; or
- large scale, systematic monitoring of public areas (CCTV)

A DPIA will provide:

- a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals; and
- the measures in place to address risk, including security and to demonstrate that you comply

A DPIA will incorporate the following steps:

1. identify the need for a PIA
2. describe the information flows
3. identify the privacy and related risks

4. identify and evaluate the privacy solutions
5. sign off and record the PIA outcomes
6. integrate the outcomes into the project plan
7. consult with internal and external stakeholders as needed throughout the process

All DPIAs must be logged centrally by emailing them to: DataProtection.Helpdesk@incommunities.co.uk

Where a DPIA indicates that personal data processing would result in a high risk (in the absence of measures taken by Incommunities/Sadeh Lok to mitigate that risk), the author of the DPIA will inform the Data Protection Officer in writing as soon as reasonably practicable. The Data Protection Officer will inform the Information Commissioner in a manner that fulfils the requirements of Article 36(3) of the GDPR.

Data Protection Impact Assessment Template

Start to fill in details from the beginning of the project. The template follows the process that is used in the Information Commissioner's Code of Practice.

Step one: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a DPIA was identified (e.g. personal data being processed).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address risks to people's privacy. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the DPIA process.

Step three: Identify the privacy and related risks

Identify the key risks to people's privacy and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

Thinking about each of the Data Protection Principles and how they could be endangered will help to identify risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to manage the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Final step: Log the DPIA by emailing it to:

DataProtection.Helpdesk@incommunities.co.uk

Signed
Name
Job title
Date

6.0 Personal Data Security

6.1 Incommunities/Sadeh Lok takes appropriate technical and organisational measures to maintain the security of personal data. The appropriateness of the measures taken is decided on a risk-based approach, with risks being assessed on impact and likelihood. The appropriate measures taken are risk treatments, which aim to bring the residual risk score down to low, which reflects Incommunities'/Sadeh Lok's risk appetite relating to personal data security.

6.2 Incommunities/Sadeh Lok aims to ensure that the confidentiality, integrity, availability and resilience of personal data processing systems are maintained without fail. This is sought to be achieved through measures such as:

- Internal policies and procedures e.g. this Data Protection Policy, the Business Continuity Plan, the ICT Code of Conduct
- External validation e.g. Cybersecurity certification, Internal Audit scrutiny, testing exercises.
- Adequate training e.g. focussed training for some roles and responsibilities, universal training via e-learning and toolbox talks.
- Suitable recruitment and selection, management, capability and disciplinary procedures to ensure that suitable staff with the rights skills/abilities/experience/attitude are trusted with the personal data Incommunities/Sadeh Lok processes.
- Board oversight e.g. annual reporting on data protection matters including data breaches to the Board, management of data protection risks via Audit & Risk Committee scrutiny.

6.3 Roles and responsibilities for personal data security

The Senior Information Risk Owner (SIRO) is a Senior Leadership Team member with overall responsibility for Incommunities'/Sadeh Lok's information risk management.

The Data Protection Officer has overall responsibility for Incommunities'/Sadeh Lok's compliance with data protection laws, and delivery of adequate advice and assistance to allow the holders of roles and responsibilities to discharge them.

The Board has overall responsibility for overseeing security of the personal that is processed.

Directors and Managers have responsibility for supervising their staff adequately to maintain personal data security, and they are the Information Asset Owners of personal data that is held and/or used by their staff.

Staff members who manage contracts are responsible for managing the data protection aspects of those contracts, including ensuring that the contractors have appropriate technical and organisational measures in place and are under a duty to report any data protection breach.

All employees have a responsibility to comply with data protection laws, Incommunities/Sadeh Lok policies, and reasonable requests from more senior employees, in order to maintain personal data security.

7.0 Document Retention Policy

7.1 Introduction

7.1.1 Retention of documents for an appropriate period of time is essential to our business, it enables us to:

- fulfil the requirements of regulatory and legal compliance
- demonstrate high standards of corporate governance
- evidence events or agreements in the case of disputes
- respond to claims or complaints
- meet day-to-day operational needs
- ensure that the organisation's decision making process is based on full, accurate and up-to-date information, as well as ensuring that the rationale for and the impact of those decisions can be traced, scrutinised and justified as necessary

7.1.2 However, the permanent retention of documents is undesirable:

- it occupies expensive storage space
- electronic systems become cluttered
- operational time and effort is diverted into managing it
- it creates an unnecessary risk of data being lost or misused

7.1.3 The GDPR regulates the ways in which all organisations are expected to collect, process, use and store personal data. Some of the records kept by Incommunities/Sadeh Lok will be personal data. The key requirements of Article 5 of the GDPR in this area are:

- data shall be adequate, relevant and limited to what is necessary in relating to the purposes for which they are processed
- data shall be accurate and, where necessary, kept up to date
- data shall not be kept for longer than is necessary

7.2 Policy scope and purpose

7.2.1 The purpose of this policy is to provide a framework within which officers can decide whether a particular document or category of documents should be either retained or destroyed.

7.2.2 The Document Retention Guidance will:

- identify documents that will be kept permanently
- prevent the destruction of documents that need to be retained for a specified period to satisfy legislative, industry, financial or other administrative requirements
- provide consistency in how documents are disposed of

- formulate Incommunities/Sadeh Lok's policy on document retention; all staff are expected to abide by this guidance
- complement Incommunities/Sadeh Lok's Data Protection Policy, which should be read in conjunction with this Guidance

7.2.3 This policy applies to all Officers and sets out the specific responsibilities of the Head of Service in the decision making process.

7.3 Retention/Disposal protocol

7.3.1 Documents which are likely to need to be retained by include:

- completed application forms
- emails – and their attachments
- letters
- invoices
- plans/drawings
- registers
- contracts;
- deeds
- financial records
- minutes

7.3.2 Documents which are unlikely to need to be kept include:

- compliment slips
- catalogues and trade journals
- telephone message slips
- non-acceptance of invitations
- trivial electronic mail messages or notes that are not related to Incommunities/Sadeh Lok business
- requests for plans or advertising material
- out of date distribution lists
- working papers that lead to a final report
- duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports, copies of documents where a hard copy has also been printed and filed

7.3.3 A decision whether to retain or dispose of a document should be taken in accordance with this protocol. The protocol requires that in making a retention/disposal decision consideration be given to the following:

- the key disposal/retention criteria: these are set out in a checklist at Appendix 1. No document should be disposed of unless these have been considered in relation to the document

- the Retention schedules at Appendix 2: these set out the mandatory or recommended retention periods for the all the categories of document likely to be encountered within Incommunities/Sadeh Lok

7.4 Document retention – roles and responsibilities

7.4.1 All officers have a responsibility for familiarising themselves with this guidance, and for ensuring that the documents they handle are processed, stored and disposed of appropriately – as far as they are able to control.

7.4.2 As operational requirements will be very different in all service areas, Directors will have the ultimate responsibility for ensuring that this Guidance is complied with within their service areas and for establishing practical systems that will enable this. Although they may delegate the operational aspects of this Guidance, they must ensure that the delegated officer is fully aware of the contents of this guidance in addition to the operational requirements of the service.

7.4.3 Directors should conduct a systematic review of documentation to be on an annual basis, disposing of any documents that are no longer required. It is advisable to complete additional and smaller scale reviews throughout the year, for example, looking through a proportion of tenant files to make certain that no personal data is being kept for longer than necessary.

7.4.4 Where Directors are in any doubt about the legality of either retaining or disposing of particular documents they should consult the Legal Services Team who can advise on minimum retention periods and whether a claim has been intimated which may require documents to be retained. Legal Services are unlikely to know whether a document needs to be retained for operational purposes; this is the responsibility of the Director of the service area.

7.5 Retention and Disposal

Retention

7.5.1 Where documents are to be retained the following principles should be followed:

- all documents should be stored systematically and enable Incommunities/Sadeh Lok to retrieve information quickly and easily
- the movement and location of documents should be controlled and leave an auditable trail
- storage facilities should be in a condition that will prevent any damage to the records. This includes ensuring that storage is safe from fire and un-authorised access, but accessible by appropriate individuals as required
- documents that require retention but are not required for day-to-day operations should where possible be stored away from offices in a secure location
- heads of Service/Operations should ensure that a contingency plan is developed for their work area to protect records that must be retained. This might include the use of back-up media that is kept off-site

Disposal

7.5.2 When a retention period has expired (as per the Schedule in Appendix 1), the Director of Service/Operations or the delegated officer should review the document and decide whether or not it should be disposed of. It is important to bear in mind that the Schedule is guidance; there may be operational circumstances where it would be sensible to retain the document longer than the recommended period.

7.5.3 The responsibility for the disposal of documents which have been scanned and stored electronically will lie with the Director/Operational Manager of ICT. To support the Director/Manager of ICT, the relevant Director of Service/Operation (or the delegated officer) should monitor electronic documents and files which relate to their service and notify ICT if they believe that the document and/or file should be destroyed.

7.5.4 Disposal may be achieved by a range of processes:

- confidential Waste disposal i.e. by placing the document within the confidential waste receptacles at each office from where it will be collected by the confidential waste disposal service engaged by Incommunities/Sadeh Lok
- physical destruction on site (e.g. by shredding paper records)
- deletion – where computer files are concerned. This requires that the data is "virtually impossible to retrieve" according to the advice issued by the Information Commissioner
- migration of a document to an external body. (This is only likely to apply where the document is a document of historical interest

8.0 Review

8.1 There will be an automatic review of this policy whenever there is a change of statutory or regulatory provisions, or when other Best Practice information becomes available that will impact on the policy. In any event there will be a substantive review of this policy every two years.

9.0 Disposal/Retention Checklist

9.1 Has the document been appraised: as a first step the nature and contents of any document being considered for retention or disposal must be appraised? This is a physical inspection of the document to establish the contents and assess which of the retention periods may be applicable.

This should be undertaken by an Officer with sufficient understanding of the operations and the corporate framework of the organisation to be able to make a decision with an appreciation of the nature and function of the document.
Any decision to the effect that all future documents of a particular description should be disposed on expiry of a specified retention period should be taken by a service Director.

9.2 Is there a legislative requirement that a document be retained for a specified period? There are in fact very few pieces of legislation which either directly or indirectly impose minimum retention periods. The most relevant are as follows:

- **Tax legislation** generally impose a minimum retention period of six years for relevant records
- **VAT records:** the VAT legislation similarly imposed a minimum retention period of six years
- **Statutory Registers:** Group organisations are from under a variety of legislation including the Companies Acts and Industrial and Provident Societies Acts. The incorporation documents and registers and records required by this legislation must be maintained permanently
- **Pension's documentation**: should generally be retained for six years after the date of retirement of any individual scheme member.

9.3 May the document be required to provide evidence in the event of a future dispute? On occasions Incommunities/Sadeh Lok becomes involved in legal disputes with third parties. Legal proceedings may be instituted against us in relation to the conduct of a letting or the repair of a property or the work done/services provided under a Contract. Conversely we may bring legal proceedings to enforce a tenancy agreement or a contract.

Where litigation arises it is essential that Incommunities/Sadeh Lok has access to all correspondence, notes and other records which are relevant to the dispute.
The Limitation Act specifies time limits for commencing legal proceedings. The starting point for document retention is the periods in the Act within which a claim must be commenced. The main time limits which are likely to be relevant are, in summary:

- claims based on a contract – 6 years from when the claim arose
- claims based on negligence – 3 years from when the claim arose
- claims based on documents under seal (i.e. deeds) – 12 years

There are two main qualifications to these periods:

- where the claim is for personal injury the period is reduced to three years Although, where the claimant is an infant or lacks legal capacity for some other reason the period is usually extended until they are of age/ regain capacity
- where the damage which is the subject of the claim hasn't become apparent for a period of time the period may be extended

9.4 Is retention required to meet the operational needs of the service? Retention may be desirable for operational reasons event though a minimum retention period has expired. This may be for future reference purposes, for precedents or for performance management (benchmarking, performance indication and comparison purposes). A professional judgment will be necessary as to the usefulness of a particular document; the requirements of the Data Protection Act should always be borne in mind.

9.5 Is retention justified because the document has historic or intrinsic value? Certain documents in the possession of the organisation may have historic interest and may be sent to the County archivist. Where it is suspected that a document may fall into this category further advice should always be taken.

Data Retention Periods Schedule

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
1	**INCORPORATION DOCUMENTS**				
1.1	Certificate of Incorporation	N/A	N/A	Permanently	Implied by CA, Sec. 13.
1.2	Certificate of change of company name	N/A	N/A	Permanently	Implied by CA, Sec. 117.
1.3	Memorandum and articles of association (original)	N/A	N/A	Permanently	Best practice
	Memorandum and articles of association (current)	Permanently	CA	Permanently	Best practice
1.5	Governance documentation	N/A	N/A	Permanently	Required for charitable status
1.6	Constitution, Aims and Objectives, rules	N/A	N/A	Permanently	Required for charitable status
1.7	Registration documentation (I&P Societies)	Permanently	IPSA	Permanently	Best practice
1.8	Certificate of Registration with the Housing Regulator	N/A	N/A	Permanently	Best practice
1.9	Confirmation letter of charitable registration	Permanently	N/A	Permanently	Best Practice
1.10	HMRC confirmation of	Permanently	N/A	Permanently	Best Practice

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
	charitable status				
1.11	Board member documents (apt letters, SLAs, bank details, etc.)	N/A	N/A	6 years after board member ceases though some details should be destroyed when membership ceases (e.g. bank details, etc.)	CA2006 recommendation for docs post termination of directorship.
2	**MEETINGS**				
2.1	Notice of meetings	N/A	N/A	6 Years	In case of challenge to validity of meeting or resolution.
2.2	Board and committee minutes	Permanently	CA	Permanently	Signed originals must be kept.
2.3	Board resolutions	Permanently	CA	Permanently	Signed originals must be kept.
2.4	Minutes and resolution of trustees (charities)	N/A	N/A	Permanently	Charity Commission CC48
3	**PARTNERSHIP MEETINGS**				
3.1	Notice of meetings	N/A	N/A	6 Years	Limitation period for legal proceedings
3.2	Partnership meeting minutes	N/A	N/A	6 Years	Limitation period for legal proceedings
3.3	Partnership resolutions	N/A	N/A	6 Years	Limitation period for legal proceedings
4	**DEMOCRATIC PROCESSES**				
4.1	Voting (Balloting Documents)	N/A	N/A	6 Years	Limitation period for legal proceedings
4.2	Voting Results (Consolidated returns of votes received)	N/A	N/A	6 Years	Limitation period for legal proceedings
5	**REGISTRATION AND STATUTORY RETURNS**				

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
5.1	Annual returns to the regulator	N/A	N/A	5 years from submission	Best practice
5.2	Annual returns to the regulator – working documents	N/A	N/A	3 years from submission	Best practice
5.3	Audited company returns and financial statements (including I&P Societies annual returns to the Registrar of Friendly Societies)	N/A	N/A	Permanently	Best practice
5.4	Declarations of interest	N/A	N/A	6 Years	Limitation for legal Proceedings.
5.5	Register of directors and secretaries	Permanently	CA	Permanently	Best practice
5.6	Register of shareholder members	Permanently	CA	Permanently	Records may be removed from register 20 years after membership ceases.
5.7	Register of seals	N/A	N/A	Permanently	Best practice
5.8	Register of shareholder certificates	N/A	N/A	Permanently	Best practice
5.9	List of Members (I&P Societies)	N/A	N/A	Permanently	Best practice
6	**STRATEGIC MANAGEMENT**				
6.1	Business plans & supporting documentation (e.g. organisation structures, aims, objectives, funding issues)	N/A	N/A	5 years after plan completion	Best practice
7	**GENERAL MANAGEMENT**				
7.1	Review of quality, efficiency, performance of service or unit e.g. best value review	N/A	N/A	5 years from closure	Best practice
7.2	Assessment of quality,	N/A	N/A	2 Years from	Best practice

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
	efficiency or performance of service or unit			closure	
7.3	Official complaints made under complaints procedure	N/A	N/A	6 years from closure	Limitation period for potential legal proceedings.
7.4	Routine responses on actions, policy or procedures	N/A	N/A	2 Years after admin use ended	Best practice
7.5	CORE logs sent to JCSHR as agents for the Housing Corp.	N/A	N/A	3 years after admin use ended	Best practice
7.6	Performance Indicator Validation Audit	N/A	N/A	5 Years after completion of audit	Best practice
8	**POLICIES, PROCEDURES, STRATEGIES**				
8.1	Evidence Files	N/A	N/A	6 years from closure	Best practice
8.2	Review of policies, procedures or strategies	N/A	N/A	6 years from closure	Best practice
9	**INSURANCES**				
9.1	Current and former policies	N/A	N/A	Permanently	Limitation can commence from knowledge of potential claim, not cause of it.
9.2	Annual Insurance schedule	N/A	N/A	6 Years	Best practice
9.3	Claims and related correspondence	N/A	N/A	3 years after settlement (allow claimant to reach 25)	Best practice
9.4	Indemnities and guarantees	N/A	N/A	6 years after expiry	Limitation for legal proceedings. 12 years if related to land.
9.5	Group health policies	N/A	`N/A	12 years after cessation of benefit	Best practice

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
9.6	Employer's liability insurance certificate	At least 40 years	Employers' Liability (Compulsory Insurance Regulations 1998)	40 Years	2008 regulations removed requirement to retain for 40 years but need to be mindful of 'long tail' industrial disease claims, etc.
10	**FINANCE, ACCOUNTING & TAX RECORDS**				
10.1	Accounting records for Limited Company	3 years	CA sec 388	6 Years	TMA Sec. 20. may require any documents relating to tax over 6 (plus) years.
10.2	Accounting records for I&P Societies	N/A	N/A	6 Years	Required by Registrar of Friendly Societies and Charity Commissioner
10.3	Balance sheets and supporting documents	N/A	N/A	6 to 10 Years	Best practice. To relate to accounting records
10.4	Loan account control reports	N/A	N/A	6 Years	Best practice
10.5	Social Housing Grant Documentation	N/A	N/A	Permanently	Best practice
10.6	Signed copy of report and accounts	N/A	N/A	Permanently	Best practice
10.7	Budgets and internal financial reports	N/A	N/A	2 Years	Best practice
10.8	Tax returns and records	N/A	N/A	10 Years	TMA Sec. 20. may require any documents relating to tax over 6 (plus) years.
10.9	VAT records	6 years	VATA	6 Years	HMRC requirement for VAT registered bodies
10.10	Orders and delivery notes	6 years	VATA	6 Years	HMRC requirement for VAT registered bodies
10.11	Copy invoices	6 years	VATA	6 Years	HMRC

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
					requirement for VAT registered bodies
10.12	Credit and debit notes	6 years	VATA	6 Years	HMRC requirement for VAT registered bodies
10.13	Cash records and till rolls	6 years	VATA	6 Years	HMRC requirement for VAT registered bodies
10.14	Journal transfer documents	6 years	VATA	6 Years	HMRC requirement for VAT registered bodies
10.15	Creditors, debtors & cash income control accounts	6 years	VATA	6 Years	HMRC requirement for VAT registered bodies
10.16	VAT related correspondence	6 years	VATA	6 Years	HMRC requirement for VAT registered bodies
10.17	Mortgages – **if signed**	6 Years	N/A	Last payment + 6 years	Limitation for legal proceedings
10.18	Mortgages – **if sealed**	12 years	N/A	Last payment + 12 years	Limitation for legal proceedings All mortgages "signed as a deed", i.e. sealed.
10.19	Right to buy	N/A	N/A	12 Years after sale of house	Best practice
10.20	Records relating to ERDF funding	N/A	N/A	12 years* *or such other time period as specified in the contract for funding	Condition of funding Even when the recommended retention date has been reached, confirmation from Government Office must be sought before records relating to ERDF funding are disposed of.

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
10.21	Records relating to NRF funding	N/A	N/A	7 Years	Best practice Records must be current
11	**OTHER BANKING RECORDS (INCLUDING GIRO)**				
11.11	Cheques	N/A	N/A	6 Years	Limitation for legal proceedings
11.12	Paying in counterfoils	N/A	N/A	6 Years	Limitation for legal proceedings
11.13	Bank statements and reconciliations	3 years (from end of financial year where transactions made)	CA	6 Years	Limitation for legal proceedings
11.14	Instructions to bank	N/A	N/A	6 Years	Limitation for legal proceedings
11.15	Rent payments	N/A	N/A	7 Years	Limitation for legal proceedings is 6 years
12	**CONTRACTS AND AGREEMENTS**				
12.1	Process of calling for expressions of interest	N/A	N/A	2 years after contract let	Best practice
12.2	The process involved in the development and specification of a contract - **Ordinary contracts (Ordinary contracts are usually <£100k)**	N/A	N/A	6 years after contract expired	Limitation for legal proceedings NB drafts leading to a final version can be destroyed
12.3	The process involved in the development and specification of a contract and EU procedures - **Contracts under seal (Contracts under seal are usually > £100k**)	N/A	N/A	12 years after contract expired	Limitation for legal proceedings NB drafts leading to a final version can be destroyed
12.4	Issuing and return of tenders	N/A	N/A	1 year after contract start	Best practice
12.5	Evaluation of tenders Ordinary **contracts**	N/A	N/A	6 Years	Limitation for legal proceedings
12.6	Evaluation of tenders **Contracts under seal**	N/A	N/A	12 Years	Limitation for legal proceedings
12.7	Unsuccessful tender	N/A	N/A	2 years after	Best practice

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
	documents			notification	
12.8	Post tender negotiation	N/A	N/A	1 year after contract expiry	Limitation for legal Proceedings
12.9	Award of contract (signed contract) **Ordinary contracts**	N/A	N/A	6 Years (including any defects liability period)	Limitation for legal Proceedings
12.10	Award of contract (signed contract) **Contracts under seal**	N/A	N/A	12 Years (including any defects liability period)	Limitation for legal Proceedings
12.11	Documents 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 – up to £10,000 NB CROSS REFER WITH FINANCIAL REGS AS THESE MAY
12.12	Publication of award notices	N/A	N/A	2 years after contract start	Best practice
12.13	Loan agreements	N/A	N/A	12 years after last payment	Limitation for legal Proceedings.
12.14	Licensing agreements	N/A	N/A	6 years after expiry	Limitation for legal Proceedings.
12.15	Rental and hire purchase agreements	N/A	N/A	6 years after expiry	Limitation for legal proceedings
12.16	Indemnities and guarantees	N/A	N/A	6 years after expiry	Limitation for legal Proceedings.
12.16	Management and amendment to contracts **Ordinary contracts**	N/A	N/A	6 years after end of contract	Limitation for legal Proceedings.
12.17	Management and amendment to contracts **Contracts under seal**	N/A	N/A	12 years after end of contract	Limitation for legal Proceedings.

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
13	**CONTRACT MANAGEMENT**				
13.1	Contract operation and monitoring	N/A	N/A	2 years after terms of contract expired	Best practice
13.2	Major works contracts – post contract documentation including site visits, resident consultation meetings and final payments	N/A	N/A	12 Years	Best Practice
14	**LEGAL**				
14.1	Case files & case file correspondence (this includes reference to day to day repairs within section 82	N/A	N/A	6 years after last action	In the case of major litigation consider permanent retention
14.2	Evidence of legal advice, as included in case files and legal correspondence	N/A	N/A	6 years after last action	Consider increased retention if related to a major precedent
14.3	Legal files relating to conveyance	N/A	N/A	12 Years	Best practice
14.4	Legal files relating to contracts under seal	N/A	N/A	20 Years	Best practice
14.5	Legal files relating to signed contracts	N/A	N/A	6 Years	Best practice
15	**CHARITABLE DONATIONS**				
15.1	Deeds of Covenant	6 years after last payment	TMA	12 years after last payment	Limitation for legal proceedings if related to land
15.2	Index of donations granted	N/A	N/A	6 Years	Best practice
15.3	Account documentation	3 years	CA	6 Years	Best practice

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
16	**APPLICATION AND TENANCY RECORDS**				
16.1	Housing Benefit notifications	N/A	N/A	6 Years	Limitation period for potential legal action
16.2	Rents statements	N/A	N/A	6 Years	Limitation period for potential legal action
16.3	Current tenants' Tenancy files, including rent payment records and details of any complaints and harassment cases	N/A	N/A	Life of tenancy + 6 years	Limitation period for potential action
16.4	Former tenants' Tenancy Files (other than tenancy agreements – see below), including rent payment records, and details of any complaints and harassment cases	N/A	N/A	6 years after termination of tenancy	Anything contained must remain compliant with the DPA
16.5	Former tenants' Tenancy Agreements and details of their leaving	N/A	N/A	6 years after termination of tenancy	Anything retained must remain compliant with the DPA
16.6	Records relating to offenders, ex offenders and persons subject to crime	N/A	N/A	While tenancy continues	Information may be held on 'need to know' basis. Police sourced records may be confidential. To be dealt with as required by police
16.7	Applications for accommodation	N/A	N/A	6 years after offer accepted	Best practice
16.8	Documentation, correspondence and information provided by other agencies relating to special	N/A	N/A	While tenancy is current	Information is held on a "need to know" basis. Medical and social services

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
	needs of current tenants				records are liable to confidential. To be passed on to relevant agency at the end of the tenancy or destroyed.
16.9	Unsuccessful housing applications			6 years after closure	Limitation period for potential legal action
16.10	Unsuccessful Right to Buy records	N/A	N/A	Life of tenancy + 6 years	Limitation period for potential legal action
16.11	Garden Assistance	N/A	N/A	4 Years	Best practice
17	**PROPERTY RECORDS**				
17.1	Rent registrations (superseded)	N/A	N/A	6 Years	
17.2	Rent registrations (not superseded)	N/A	N/A	Permanently	
17.3	Fair rent documentation	N/A	N/A	6 Years	Rent officer recommendation
17.4	Leases and deeds of ownership	N/A	NCVO	While owned. Deeds of title permanently or until property disposed of. Leases – 15 years after expiry	Best practice
17.5	Copy of former leases	N/A	N/A	15 years after expiry of lease and settlement of all issues	Limitation for legal action relating to land or contracts under seal is 12 years.
17.6	Current lessee files	N/A	N/A	Indefinitely	Best Practice
17.7	Former lessee files	N/A	N/A	12 years after settlement of all issues	Best Practice
17.8	Wayleaves, licences and easements	N/A	N/A	12 years after right given or	Limitation for legal action

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
				received cease	relating to land or contracts under seal
17.9	Abstracts of titles	N/A	N/A	12 years after interest ceases	Limitation for legal action relating to land or contracts under seal
17.10	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
17.11	Searches	N/A	N/A	12 years after interest ceases	Limitation for legal action relating to land or contracts under seal
17.12	Property maintenance records and inspections (includes actions carried out whilst property is empty)	N/A	N/A	6 Years	Limitation for legal action
17.13	Reports and professional opinions	N/A	N/A	6 Years	Limitation for legal action
17.14	Development documentation	N/A	N/A	12 years after settlement of all issues	Limitation for legal action relating to land or contracts under seal
17.15	Invoices	6 years	VAT Act	12 Years	Limitation for legal action relating to land or contracts under seal
17.16	RTB Sales Administration (not including Plans for Sale)	N/A	N/A	Permanently	These are currently scanned, with hard copies disposed of
17.17	Details of asbestos	N/A	N/A	Permanently	Best practice
17.18	Waste transfer notes	N/A	N/A	3 Years	Best practice
17.19	Pest control treatment reports and risk assessments	N/A	N/A	3 Years	Best practice

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
17.20	Completed job sheets – voids/ 1 off cleans/ Lumia	N/A	N/A	2 Years	Best practice
17.21	Completed job sheets – Tree works	N/A	N/A	4 Years	Best practice
17.22	Playground check sheets	N/A	N/A	21 Years	Best practice
17.23	Needles check sheet	N/A	N/A	As long as you hold a permit	Best practice
17.24	Weedkilling records	N/A	N/A	4 Years	Best practice
18	**PUBLIC CONSULTATION**				
18.1	Consultation documents	N/A	N/A	Five years from closure	Best practice
18.2	Consolidated consultation returns	N/A	N/A	Five years from closure	Best practice
19	**PUBLICATIONS**				
	Job database	N/A	N/A	Five years from last action on paper and permanently in electronic form	Best practice
20	**MEDIA RELATIONS & MARKETING**				
20.1	Written responses and releases to the media	N/A	N/A	Three years from closure	Best practice
20.2	Media cuttings	N/A	N/A	Permanently	Best practice
20.3	Details of Incommunities promotions – Brand Portfolios	N/A	N/A	Permanently	Best practice
21	**VEHICLES**				
21.1	Mileage records	N/A	N/A	2 years after disposal	Best practice
21.2	Maintenance records, MOT tests	N/A	N/A	2 years after disposal	Best practice

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
21.3	Vehicle check sheets	N/A	N/A	2 years after disposal	Best practice
21.4	Copy registrations	N/A	N/A	2 years after disposal	Best practice
22	**EMPLOYEES: TAX AND SOCIAL SECURITY**				
22.1	Records of taxable payments	6 years	TMA	6 Years	HMRC require retention of each payment for 3 years
22.2	Record of tax deducted or refunded	6 years	TMA	6 Years	HMRC require retention of each payment for 3 years
22.3	Record of earnings on which standard National Insurance Contributions Payable	6 years	TMA	6 Years	HMRC require retention of each payment for 3 years
22.4	Record of employer's and employee's National Insurance Contributions	6 years	TMA	6 Years	HMRC require retention of each payment for 3 years
22.5	NIC contracted –out arrangements	6 years	TMA	6 Years	
22.6	Copies of notices to employee (E.g. P45, P60)	6 years	TMA	6 years plus current year	
22.7	HMRC notice of code of changes, pay & tax details	6 years	TMA	6 Years	
22.8	Expense claims	N/A	N/A	6 years after audit	Best practice
22.9	Payments made by staff for personal calls from a works mobile	N/A	N/A	1 Year	Best practice
22.10	Sick Notes	N/A	N/A	6 years after employment	Best practice
22.11	Record of sickness payments	3 years following year to which they relate	SSPR	3 Years	Inland Revenue require retention of each payment for 3 years
22.12	Record of maternity/adoption payments	3 years following year to which they relate	SSPR	3 Years	HMRC require retention of each payment for 3 years

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
22.13	Income tax and NI returns	3 years following year to which they relate	IT(E)R	6 Years	Best practice
22.14	Redundancy details and record of payments & refunds	N/A	N/A	12 Years	Chartered Institute of Personnel and Development (CIPD) recommendation
22.15	HMRC approvals	N/A	N/A	Permanently	CIPD recommendation
22.16	Annual earnings summary	N/A	N/A	12 Years	Best practice
23	**EMPLOYEES: PENSION SCHEMES**				
23.1	Actuarial valuation reports	N/A	N/A	Permanently	CIPD recommendation
23.2	Detailed returns of pension fund contributions	N/A	N/A	Permanently	Best practice
23.3	Annual reconciliations of fund contributions	N/A	N/A	Permanently	Best practice
23.4	Money purchase details	N/A	N/A	6 years after transfer or value taken	CIPD recommendation
23.5	Qualifying service details	N/A	N/A	6 years after transfer or value taken	CIPD recommendation
23.6	Investment policies	N/A	N/A	12 years from end of benefits payable under policy	CIPD recommendation
23.7	Pensioner records	N/A	N/A	12 years after benefits cease	CIPD recommendation
23.8	Records relating to retirement benefits (including decisions to allow retirement due to incapacity, pension accounts and associated documents)	6 years after year of retirement	RBS (IP) R	6 years after year of retirement	Statutory requirement
24	**EMPLOYEES (PERSONNEL PROCEDURES)**				

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
24.1	Personnel files (including training records and disciplinary records)	N/A	N/A	6 years after employment ceases	CIPD recommendation
24.2	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 payment	Limitation for legal proceedings
24.3	Service contracts for directors (companies)	3 years	CA	6 years after directorship ceases	Best practice
24.4	Remuneration package	N/A	N/A	6 years after last date of currency	Common practice
24.5	Former employees' Personnel Files	N/A	N/A	6 years after date of termination	CIPD recommendation
24.6	References to be provided for former employees	N/A	N/A	20 Years	Best practice
24.7	Shortlists, interview notes and related application forms	N/A	N/A	1 Year	CIPD recommendation
24.8	Application forms of non-short listed candidates	Three months after notification	SDA & RRA	1 Year	Although the Commission for Racial Equality and Equal Opportunities Commission recommends 6 months, the CIPD recommends a retention period of 1 year
24.9	Time sheets	N/A	N/A	1 year	Best practice
24.10	Trade union agreements	N/A	N/A	10 Years after ceasing to be effective	CIPD recommendation
24.11	Trust deeds, rules and	N/A	N/A	Permanently	CIPD

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
	minutes (for joint employee/employer sports/social clubs, etc, set up under trust)				recommendation
24.12	CRB (Now DBS) clearance notification	Date of clearance and up to maximum of 6 months		Date of clearance and up to maximum of 6 months	DBS check code of practice (Home Office)
24.12	Employer/employee committee minutes	N/A	N/A	Permanently	CIPD recommendation
24.13	Financial rewards			7 years after action completed	
25	**EMPLOYEES: DISCIPLINARY**				
25.1	Oral warning – 6 months	N/A	N/A	6 years after employment ceases	CIPD recommendation (part of personnel file) Must be disregarded for disciplinary purposes after time spent (6 months) and stored confidentially
25.2	Written warning – 1 year	N/A	N/A	6 years after employment ceases	CIPD recommendation (part of personnel file) Must be disregarded for disciplinary purposes after time spent (1 year) and stored confidentially
25.3	Final warning – 18 months	N/A	N/A	6 years after employment ceases	CIPD recommendation (part of personnel file)

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
					Must be disregarded for disciplinary purposes after time spent (1 year) and stored confidentially
25.4	Warnings involving children	N/A	N/A	Permanently	Incommunities does not employ anyone to work specifically with children. If this situation arises the advice of the Legal Team should be sought.
25.5	Termination/Redundancy (including calculation of payments, refunds and notification to the Secretary of State)	N/A	N/A	6 years after termination/ redundancy	If a pension is paid then records should be destroyed six years after the last payment of the pension
26	**EMPLOYEES: TRAINING**				
26.1	Training programmes	N/A	N/A	6 years after completion	Best practice
26.2	Individual training records	N/A	N/A	6 years after employment ceases	Best practice
26.3	Training –occupational health and safety	N/A	N/A	50 Years after training completed	Best practice
26.4	Tool box talk – attendance record	N/A	N/A	Life of the Personnel file	Best practice
27	**EMPLOYEES: HEALTH AND SAFETY**				
27.1	Medical records relating to control of and exposure to asbestos (and medical examination certificates)	40 years from the date of last entry (and 4 years from the date of issue)	CAWR	40 Years	Best practice
27.2	Medical records and	40 years	CLWR	40 Years	Best practice

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
	details of biological tests under the CLWR 1998	from the date of last entry			
27.3	Medical records under the IRR 1999	Until the person reaches 75 years of age, but for a minimum of 50 years	IRR 1999	50 Years	Best practice
27.4	Records of tests and examinations of control systems and protective equipment under the COSHH 1999	5 years from the date the tests were carried out	COSHH 1999	5 years from the date the tests were carried out	Best practice
27.5	Health and Safety assessments	N/A	N/A	Permanently	CIPD recommendation
27.6	Health and Safety policy statements	N/A	N/A	Permanently	Good practice
27.7	Records of consultations with safety representatives	N/A	N/A	Permanently	CIPD recommendation
27.8	Accident records, reports	3 years after date of occurrence	RIDDOR	6 years after date of occurrence 25 years for children	Limitation for legal proceedings
27.9	Accident books	N/A	N/A	6 years after date of last entry	Limitation for legal proceedings
27.10	Sickness records (including self certificates)	3 years after the end of the tax year to which they relate	SSPR	6 years from end of sickness	Limitation for legal proceedings
27.11	Health and safety statutory notices	N/A	N/A	6 years after compliance	Limitation for legal proceedings
27.12	Process of checking and ensuring the health of staff	N/A	N/A	75 years after DOB	Best practice
27.13	HAVS	N/A	N/A	40 Years	Best practice
27.14	Machine service records	N/A	N/A	10 Years	Best practice

	Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
28	**EMPLOYEES: HEALTH AND SAFETY**				
28.1	Performance monitoring	N/A	N/A	5 Years after action completed	Best practice
28.2	28.2 Monitoring of leave and attendance	N/A	N/A	2 Years after action completed	Best practice

KEY TO STATUTORY RETENTION SOURCES	
CA	Companies Act 2006
CAWR	Control of Asbestos at Work Regulations 1987
Ch A	Children's Act 1989
CLWR	Control of Lead at Work Regulations 1998
COSHH	The Control of Substances Hazardous to Health Regulations 1999
IRR	The Ionising Radiations Regulations 1999
IT(E)R	Income Tax (Employment) Regulations 1993
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1985
RBS(IP)R	Retirement Benefits Schemes (Information Powers) Regulations 1995
RRA	Race Relation Act 1976
SDA	Sex Discrimination Act 1965 & 1975
SMPR	Statutory Maternity Pay Regulations 1982
SSPR	Statutory Sick Pay Regulations 1982
TMA	Taxes Management Act 1970
VATA	Value Added Tax Act 1994

10.0 Records management

10.1 Records management ensures the systematic management of all records and the information they contain throughout their lifecycle. It is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Incommunities/Sadeh Lok's records management will:

- meet all of Incommunities/Sadeh Lok' internal business needs
- enable the content of the record to be accessed, used and reused in a controlled and efficient manner
- be compliant with all regulatory and statutory requirements
- be capable of providing evidence of a transaction or business process which is admissible in a court of law
- ensure records are kept and maintained/stored in the most appropriate way consistent with the above
- ensure records are disposed of in a way which is auditable, and meets all
- environmental and other requirement

10.2 Creating records

Creating records which contain all relevant content and contextual information not only ensures that the transaction in question has been fully and appropriately documented, but also that the record has value as a source of information to others. Any 'record' which has parts of its content missing, or is otherwise incomplete, will clearly not be reliable. Incomplete records not only reduce their informational value, they can also prove to be positively misleading and potential dangerous. The user may not be aware of important additional information, amendments or clarifications which may fundamentally alter the meaning of the record. This may lead to well-meaning but incorrect decisions being made based on false assumptions.

You create a complete record by keeping all key documents and/or media that explain how a decision was reached on a registered file. This can include (but is not limited to) correspondence, submissions, evidence, emails, court documents, internal memos, film, presentations, spreadsheets, minutes, agendas, business papers, reports, audio recordings, transcripts, press releases, web pages, policies, guidance and announcements. With regard to emails the entire chain of emails forms the record.
Incommunities/Sadeh Lok's records are created, stored and recalled from various record management systems across the business.

10.3 Maintaining records

Records must be maintained. This does not require every record to be checked onerously on a periodic basis , just in case something has changed. It involves updating and correcting records where we become aware that the information in that record is not adequate and/or accurate any more. The responsibility for

updating and correcting records rests with the person who is handling that record at the relevant time.

10.4 Retaining or destroying records

Please refer to the document retention section of this Data Protection Policy.

11.0 Monitoring Employees Policy & Procedure

11.1 Incommunities/Sadeh Lok has to monitor employees generally and, on occasion, specifically. Reasons for such monitoring may include:

- protecting the health and safety of the monitored employees, other employees and/or the general public
- building a case for HR procedures such as disciplinary or capability e.g. an employee routinely arrives at work late, which may lead to monitoring of when they are filmed on CCTV entering the building and/or checking what time they log on to the IT system

11.2 Monitoring employees affects their privacy but can be undertaken if justified. Incommunities/Sadeh Lok has adopted the Information Commissioner's guidance and procedure on monitoring employees, which may be changed from time to time by the Information Commissioner. The relevant guidance and procedure can be found at www.ico.org.uk.

12.0 Restrictions to the Exercise of Individual Rights and Restrictions to the Communication of a Personal Data Breach to the Person Whose Data Was Involved

12.1 The exercise of individual rights (e.g. subject access requests), and the duty to inform a person whose data was involved in a data breach, may be restricted if such a restriction respects the spirit of the fundamental rights and freedoms, and is a necessary and proportionate restriction to protect:

- protecting third parties' privacy rights
- national security (e.g. extremism investigations)
- public security (e.g. large scale public order problems)
- the prevention, investigation, detection or prosecution of crime including the fulfilment of a criminal penalty (e.g. tackling serious ASB)
- the general public interest in administering the social security system effectively (e.g. Income Team's communication with the Department for Work and Pensions)
- the prevention, investigation, detection or prosecution of regulatory breaches by regulated professions (e.g. reporting a breach of ethics by an opponent solicitor to their regulator)
- monitoring the exercise of official authority (e.g. Bradford Metropolitan District Council undertaking oversight of Incommunities/Sadeh Lok issuing Community Protection Notices);
- the enforcement of civil claims (e.g. possession proceedings or employment law disputes).

The above list covers the restrictions most relevant to Incommunities/Sadeh Lok. Advice should always be obtained from the Data Protection Helpdesk before exercising one of these restrictions.

12.2 There will be a review of this policy whenever there is a fundamental change of legislative or regulatory provisions, or when other information becomes available that will impact on the policy, such as the outcome of a service review. Irrespective of this, there will be a review of the policy every three years.

13.0 Data Protection Breach Management Policy & Procedure

13.1 Introduction

The Data Security Principle of the GDPR (Article 5(f)) requires that personal data is 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.

A data protection breach is 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. Data protection breaches can be categorised as one or more of the following three types:

- confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data
- integrity breach - where there is an unauthorised or accidental alteration of personal data
- availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data

Despite the appropriate technical and organisational measures we adopt, we understand that occasionally data protection breaches occur. When they occur, we will use the following four stage process:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

13.2 Containment and recovery

The Data Protection Officer (DPO) or their delegate will lead the investigation; however, the requested assistance of any member of staff is compulsory.
The DPO or their delegate will decide what action needs to be taken to contain the data protection breach. Example actions include requesting a third party who intentionally or inadvertently holds personal data does not read it or disseminate it further, reporting any criminal offence to the Police, or threatening legal action to deter further dissemination of personal data that is now outside of our control otherwise.

The DPO or their delegate will decide what action needs to be taken to recover the personal data lost, stolen or destroyed by the data protection breach. Example actions include requesting a document is returned or destroyed, threatening legal action against a third party who intentionally or inadvertently holds personal data and refuses to return it, or using back up data to restore lost data.

13.3 Assessment of ongoing risk

The DPO or their delegate will assess the ongoing risk by considering all of the circumstances. The following questions may be useful for this risk assessment. The initial risk will be treated, which will result in a residual risk. The impact of the risk and the probability of it occurring should be assessed at both the initial risk and residual risk stage:

- what type of data is involved?
- how sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details).
- if data has been lost or stolen, are there any protections in place such as encryption?
- what has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
- regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people, to be used to perpetrate a fraud.
- how many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.
- who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks.
- what harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- have individuals' bank details have been lost? If so, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.
- what risk treatment is possible? What risk treatment is reasonable in light of the initial assessed risk?

The risk assessment following a breach is important for two reasons. First, it is vital to the effective management of the risk created by a data protection breach. Secondly, it is integral to the decision on whether to notify the ICO and/or the affected individuals.

13.4 Notification of breach

We will notify the Information Commissioner (ICO) of a personal data breach within 72 hours of becoming aware of it and sooner where practicable, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals.

The breach notification to the ICO will:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by us to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- where it is not possible to provide the above information at the same time, the information may be provided in phases as soon as practicable.

We will notify the individual(s) whose personal data is subject of the breach as soon as practicable when the personal data breach is likely to result in a high risk to the rights and freedoms of the individual(s). The assessment of risk will include taking into account technical or organisational taken before or after the breach, which result in the risk not being high risk (e.g. encryption making the personal data unintelligible). Notification of the breach is subject to the Restrictions section of this policy.

The breach notification to the individual(s) will describe in clear and plain language the nature of the personal data breach and will:

- communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by us to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If issuing breach notifications to each individual would involve disproportionate effort, we will instead make a public communication or similar measure whereby the informed are informed in an equally effective manner (e.g. local media announcement and website article).

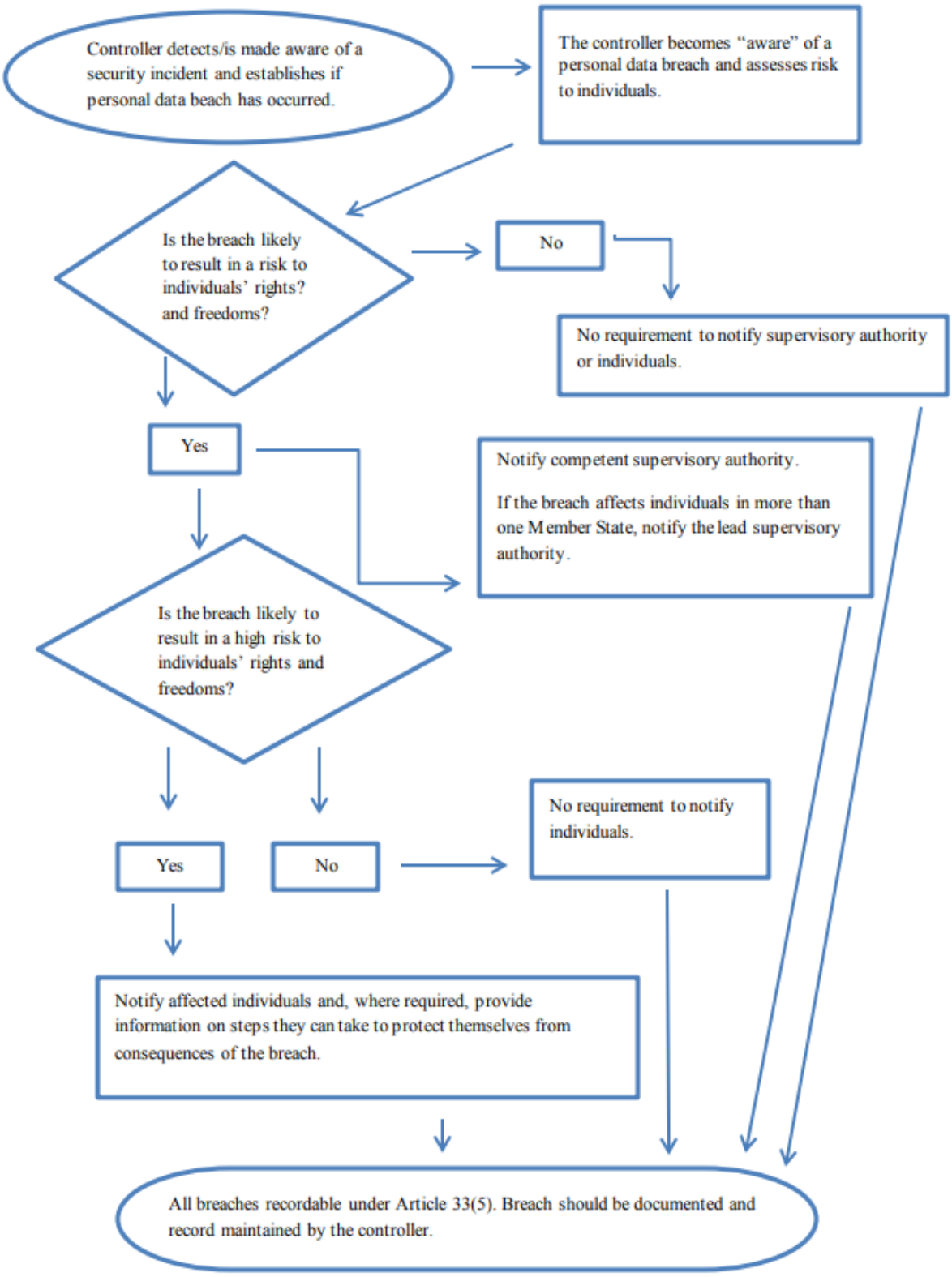
13.5 Evaluation and response

The DPO or their delegate will evaluate the causes of the data protection breach, the circumstances leading to its discovery and how the breach was handled under the Data Protection Breach Management Procedure. This will completed in order to recommend and implement appropriate technical or organisational measures to reduce the risk of a repeat of the breach and its impact if it does occur.

13.6 Record-keeping

The DPO or their delegate will document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the ICO to verify compliance and Incommunities Group Ltd Board to receive an annual report on data protection compliance including breaches and how they were handled.

A. Flowchart showing notification requirements



14.0 Data Protection Training Policy & Procedure

14.1 All staff who may have access to personal data will receive induction training on their Data Protection responsibilities.

14.2 All staff who may have access to personal data will receive refresher training on their Data Protection responsibilities at least once every two years.

14.3 Training will be provided either by way of information presentation sessions or via e-learning.

14.4 It is the responsibility of all staff who deal with personal data to ensure that they access training events and/or complete e-learning modules (as appropriate) and that they are ware of their obligations under this Policy. Where refresher training is to be provided by e-learning, managers must ensure that employees in their team have access to electronic resources in order to complete the training.

15.0 Subject Access Requests Policy & Procedure

15.1 Rights

The GDPR gives individuals the following rights:

- confirmation of whether or not their personal data is being processed;
- the purpose of the processing;
- the recipients of disclosed personal data;
- the envisaged retention period;
- confirmation of the rights to rectification and erasure;
- confirmation of the right to complain to the Information Commissioner;
- explanation of the source of the data, if it was not the data subject;
- the existence of automated decision-making and the underlying logic.

The exercise of this right is subject to the Restrictions section of this policy.

15.2 Recognising a subject access request

All staff members receive adequate data protection training to recognise a subject access request when it is made. A staff member must inform the Data Protection Helpdesk that a subject access request has been made as soon as reasonably practicably. It is important to remember that subject access requests are often incorrectly named ‘freedom of information requests’ or similar. A subject access request can be recognised if it is a person asking for their own data.

15.3 Responsibility

It is the responsibility of the recipient of the subject access request to fulfil it. It is the responsibility of the Data Protection Officer to advise and assist; the level of advice and assistance is at the discretion of the Data Protection Officer. It is the responsibility of all staff members to assist the recipient and the Data Protection Officer in handling subject access requests.

15.4 Sufficiency of the request

A subject access request must be sufficiently clear to enable the information to be found. If it is not sufficiently clear, the recipient should seek clarification as soon as practicable. The time limit does not start running until a sufficiently clear request has been received.

15.5 Proving identity

Often, the recipient of a subject access request will be sure of the identity of the requestor i.e. they will receive the request from a recognised email address, or the request will ask the data to be sent by post to a recognised home address. Where the recipient has doubts over the identity of the requestor, they should seek adequate proof. This may be as simple as asking the requestor to clarify their name, date of birth, home address etc., or it may require the requestor to provide identification such as photo ID (driving licence, passport) and a recent utility bill showing their address. The time limit does not start running until the requestor's identity is certain to the recipient.

15.6 Time limits

Generally, subject access requests should be concluded within one calendar month of receipt. The Data Protection Officer manages a tracker which monitors this. It is the responsibility of the recipient to ensure the time limit is met. If the subject access request is particularly complex, the time limit can be extended by up to two further months but this should only be done with the Data Protection Officer's authorisation because it may need to be justified to the Information Commissioner in the event of a complaint by the requestor. The requestor must also be informed in writing of the extension and the reason for it.

15.7 Fees

No fees can be charged to fulfil a subject access request, subject to the provisions on manifestly unfounded or excessive subject access requests.

15.8 Manifestly unfounded or excessive subject access requests

On occasion, subject access requests are manifestly unfounded or excessive. If this is suspected, the Data Protection Officer will determine whether Incommunities/Sadeh Lok regards the particular subject access request as manifestly unfounded or excessive. If such a determination is made, the Data Protection Officer will decide whether to charge a reasonable fee (the rule of thumb is £250 to cover the labour costs and administration costs of fulfilling the request) or to refuse the request.

15.9 Collation of data and the communication with the requestor

The communication with the requestor will be by letter if a letter was received or by email if an email was received, unless the requestor specifies a preference for email or letter. The communication will answer each of the rights a requestor has (listed at the beginning of this section) and provide the data (which may be redacted in accordance with recognised exemptions such as protecting third party data, commercially sensitive data etc.).

15.10 Concluding a subject access request

When the communication concluding the subject access request is sent to the requestor, this must also be sent to the Data Protection Helpdesk. This step allows a copy of the concluding communication to be stored centrally and for the tracker to be updated.

16.0 Right to be Forgotten Policy & Procedure

16.1 Right to be forgotten

A person has the right to be forgotten in certain circumstances. These are:

- the personal data was collected for purposes which no longer apply
- the person withdraws their consent and no other legal grounds for processing exist
- the person objects to the processing under Article 21 of the GDPR and no overriding legitimate grounds for the processing exist
- the person objects to processing for direct marketing
- the personal data have been unlawfully processed
- the personal data have to be erased to comply with a legal obligation

The exercise of this right is subject to the Restrictions section of this policy.

If the personal data has been made public by Incommunities/Sadeh Lok, we shall take reasonable steps (taking into account cost and technological capability) to inform other data controllers who are processing the data of the person's erasure request.

The right to be forgotten does not apply where processing is necessary:

- to bring or defend legal claims;
- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- to protect public health in the public interest;
- to allow scientific, historical or statistical archiving.

16.2 Recognising a right to be forgotten request

These will usually be fairly obvious as they will use words such as 'right to be forgotten', 'erasure' or 'delete'. If a recipient receives a right to be forgotten request, or is unsure if a communication is such a request, it must be referred to the Data Protection Helpdesk as soon as reasonable practicable.

16.3 Responsibility

It is the responsibility of the recipient to forward the request to be forgotten to the Data Protection Helpdesk. Once the request is received at the Data Protection Helpdesk, it is the Data Protection Officer's responsibility to handle the request. It is the responsibility of all staff members to assist the Data Protection Officer in handling such request.

16.4 Sufficiency of the request

A request must be sufficiently clear to enable the decision on whether to erase the personal data to be handled.. If it is not sufficiently clear, the recipient should seek clarification as soon as practicable. The time limit does not start running until a sufficiently clear request has been received.

16.5 Proving identity

Often, the recipient of a request to be forgotten will be sure of the identity of the requestor i.e. they will receive the request from a recognised email address, or the request will ask the data to be sent by post to a recognised home address. Where the recipient has doubts over the identity of the requestor, they should seek adequate proof. This may be as simple as asking the requestor to clarify their name, date of birth, home address etc., or it may require the requestor to provide identification such as photo ID (driving licence, passport) and a recently utility bill showing their address. The time limit does not start running until the requestor's identity is certain to the recipient.

16.6 Time limits

Generally, requests to be forgotten should be concluded within one calendar month of receipt. The Data Protection Officer manages a tracker which monitors this. It is the responsibility of the Data Protection Officer to ensure the time limit is met. If the request to be forgotten is particularly complex, the time limit can be extended by up to two further months but this should only be done with the Data Protection Officer's authorisation because it may need to be justified to the Information Commissioner in the event of a complaint by the requestor. The requestor must also be informed in writing of the extension and the reason for it.

16.7 Fees

No fees can be charged to fulfil a request to be forgotten, subject to the provisions on manifestly unfounded or excessive requests.

16.8 Manifestly unfounded or excessive requests

On occasion, requests to be forgotten are manifestly unfounded or excessive. If this is suspected, the Data Protection Officer will determine whether Incommunities/Sadeh Lok regards the particular request as manifestly unfounded or excessive. If such a determination is made, the Data Protection Officer will decide whether to charge a reasonable fee (the rule of thumb is £250 to cover the labour costs and administration costs of fulfilling the request) or to refuse the request.

16.9 Communication with third parties to whom the personal data has been disclosed

If the request is to be followed, the Data Protection Officer will communicate via letter or email with any recipient to whom the personal data has been disclosed, unless this would be impossible or would involve disproportionate effort. This communication will inform the third party of the erasure.

16.10 Communication with the requestor

The Data Protection Officer will communicate with the requestor via letter or email to inform them whether their request has been followed and, if not, the reasons why. The Data Protection Officer will then update the tracker.

17.0 Right to Data Portability Policy & Procedure

17.1 Right to receive personal data

A person has the right to receive their personal data held by Incommunities/Sadeh Lok and/or have that personal data transmitted to a third party (where technically feasible), subject to the requirements below.

17.2 Right to data portability

The right to data portability only applies if the processing is based on consent or a contract, and the processing is carried out by automated means.

17.3 Transmitting data

If the data is to be transmitted, it must be done so in a structured, commonly used and machine-readable format.

17.4 Right to be forgotten

If the person has also exercised their right to be forgotten, both rights can be met alongside each other. The exercise of this right is subject to the Restrictions section of this policy.

17.5 Recognising a right to data portability request

These will usually be fairly obvious as they will expressly ask for their personal data to be transmitted to a third party. If a recipient receives a request, or is unsure if a communication is such a request, it must be referred to the Data Protection Helpdesk as soon as reasonable practicable.

17.6 Responsibility

It is the responsibility of the recipient to forward the request to the Data Protection Helpdesk as soon as reasonably practicable. Once the request is received at the Data Protection Helpdesk, it is the Data Protection Officer's responsibility to handle the request. It is the responsibility of all staff members to assist the Data Protection Officer in handling such request.

17.7 Sufficiency of the request

A request must be sufficiently clear to determine whether the right to data portability applies. If it is not sufficiently clear, the recipient should seek clarification as soon as practicable. The time limit does not start running until a sufficiently clear request has been received.

17.8 Proving identity

Often, the recipient of a request exercising the right to data portability will be sure of the identity of the requestor i.e. they will receive the request from a recognised email address, or the request will ask the response to be sent by post to a recognised home address. Where the recipient has doubts over the identity of the requestor, they should seek adequate proof. This may be as simple as asking the requestor to clarify their name, date of birth, home address etc., or it may require the requestor to provide identification such as photo ID (driving licence, passport) and a recently utility bill showing their address. The time limit does not start running until the requestor's identity is certain to the recipient.

17.9 Time limits

Generally, requests should be concluded within one calendar month of receipt. The Data Protection Officer manages a tracker which monitors this. It is the responsibility of the Data Protection Officer to ensure the time limit is met. If the request is particularly complex, the time limit can be extended by up to two further months but this should only be done with the Data Protection Officer's authorisation because it may need to be justified to the Information Commissioner in the event of a complaint by the requestor. The requestor must also be informed in writing of the extension and the reason for it.

17.10 Fees

No fees can be charged to fulfil a request to exercise the right to data portability, subject to the provisions on manifestly unfounded or excessive requests.
Manifestly unfounded or excessive requests

On occasion, requests to restrict processing are manifestly unfounded or excessive. If this is suspected, the Data Protection Officer will determine whether Incommunities/Sadeh Lok regards the particular request as manifestly unfounded or excessive. If such a determination is made, the Data Protection Officer will decide whether to charge a reasonable fee (the rule of thumb is £250 to cover the labour costs and administration costs of fulfilling the request) or to refuse the request.

17.11 Communication with the requestor

The Data Protection Officer will communicate with the requestor via letter or email to inform them whether their request has been followed and, if not, the reasons why. The Data Protection Officer will then update the tracker.

18.0 Right to Object Policy & Procedure

18.1 Right to object

A person shall have the right to object to Incommunities/Sadeh Lok from processing that person's personal data in the following circumstances:

- if the legitimate interest justification is being relied upon;
- if the official authority justification is being relied upon (rarely used by Incommunities/Sadeh Lok); or

- if Incommunities/Sadeh Lok is processing the personal data for direct marketing.

The exercise of this right is subject to the Restrictions section of this policy.

18.2 Recognising a right to object request

These will usually be fairly obvious as they will expressly state that they object to the processing or they want the processing/direct marketing to stop. If a recipient receives a request, or is unsure if a communication is such a request, it must be referred to the Data Protection Helpdesk as soon as reasonable practicable.

18.3 Responsibility

It is the responsibility of the recipient to forward the request to the Data Protection Helpdesk as soon as reasonably practicable. Once the request is received at the Data Protection Helpdesk, it is the Data Protection Officer's responsibility to handle the request. It is the responsibility of all staff members to assist the Data Protection Officer in handling such request.

An objection to processing of personal data under the legitimate interest and/or official authority justification will be allows unless:

- Incommunities/Sadeh Lok can demonstrate compelling legitimate grounds for the processing which override the person's privacy rights; or
- the processing is necessary for the establishment, exercise or defence of legal claims

18.4 Sufficiency of the request

A request must be sufficiently clear to enable the decision on whether to allow the request to be handled. If it is not sufficiently clear, the recipient should seek clarification as soon as practicable.

18.5 Proving identity

Often, the recipient of a request will be sure of the identity of the requestor i.e. they will receive the request from a recognised email address, or the request will ask the response to be sent by post to a recognised home address. Where the recipient has doubts over the identity of the requestor, they should seek adequate proof. This may be as simple as asking the requestor to clarify their name, date of birth, home address etc., or it may require the requestor to provide identification such as photo ID (driving licence, passport) and a recently utility bill showing their address. The time limit does not start running until the requestor's identity is certain to the recipient.

18.6 Time limits

Generally, requests to exercise the right to object should be concluded as soon as practicable. The Data Protection Officer manages a tracker which monitors this. It is the responsibility of the Data Protection Officer to ensure the time limit is met.

18.7 Fees

No fees can be charged.

18.8 Manifestly unfounded or excessive requests

On occasion, requests are manifestly unfounded or excessive. If this is suspected, the Data Protection Officer will determine whether Incommunities/Sadeh Lok regards the particular request as manifestly unfounded or excessive. If such a determination is made, the Data Protection Officer will refuse the request.

18.9 Communication with third parties to whom the personal data has been disclosed

If the request is to be followed, the Data Protection Officer will communicate via letter or email with any recipient to whom the personal data has been disclosed, unless this would be impossible or would involve disproportionate effort. This communication will inform the third party of the exercise of the right to object and Incommunities/Sadeh Lok's decision.

18.10 Communication with the requestor

The Data Protection Officer will communicate with the requestor via letter or email to inform them whether their request has been followed and, if not, the reasons why. The Data Protection Officer will then update the tracker.

19.0 Right to Rectification Policy & Procedure

19.1 Right to rectification

A person has the right to have their inaccurate personal data held by Incommunities/Sadeh Lok rectified. This includes having incomplete personal data completed, including by them providing a supplementary statement.

The exercise of this right is subject to the Restrictions section of this policy.

19.2 Recognising a right to rectification request

These will usually be fairly obvious as they will expressly state that they want inaccurate or incomplete personal data to be corrected. If a recipient receives a request, or is unsure if a communication is such a request, it must be referred to the Data Protection Helpdesk as soon as reasonable practicable.

19.3 Responsibility

It is the responsibility of the recipient of the request to fulfil it. It is the responsibility of the Data Protection Officer to advise and assist; the level of advice and assistance is at the discretion of the Data Protection Officer. It is the responsibility of all staff members to assist the recipient and the Data Protection Officer in handling right to rectify requests.

19.4 Sufficiency of the request

A request must be sufficiently clear to enable the decision on whether to rectify the personal data. If it is not sufficiently clear, the recipient should seek clarification as soon as practicable. The time limit does not start running until a sufficiently clear request has been received.

19.5 Proving identity

Often, the recipient of a request to rectify personal data will be sure of the identity of the requestor i.e. they will receive the request from a recognised email address, or the request will ask the response to be sent by post to a recognised home address. Where the recipient has doubts over the identity of the requestor, they should seek adequate proof. This may be as simple as asking the requestor to clarify their name, date of birth, home address etc., or it may require the requestor to provide identification such as photo ID (driving licence, passport) and a recently utility bill showing their address. The time limit does not start running until the requestor's identity is certain to the recipient.

19.6 Time limits

Generally, requests to rectify personal should be concluded within one calendar month of receipt. The Data Protection Officer manages a tracker which monitors this. It is the responsibility of the Data Protection Officer to ensure the time limit is met. If the request is particularly complex, the time limit can be extended by up to two further months but this should only be done with the Data Protection Officer's authorisation because it may need to be justified to the Information Commissioner in the event of a complaint by the requestor. The requestor must also be informed in writing of the extension and the reason for it.

19.7 Fees

No fees can be charged to fulfil a request to rectify personal data, subject to the provisions on manifestly unfounded or excessive requests.

19.8 Manifestly unfounded or excessive requests

On occasion, requests to rectify personal data are manifestly unfounded or excessive. If this is suspected, the Data Protection Officer will determine whether Incommunities/Sadeh Lok regards the particular request as manifestly unfounded or excessive. If such a determination is made, the Data Protection Officer will decide whether to charge a reasonable fee (the rule of thumb is £250 to cover the labour costs and administration costs of fulfilling the request) or to refuse the request.

19.9 Communication with third parties to whom the personal data has been disclosed

If the request is to be followed, the Data Protection Officer will communicate via letter or email with any recipient to whom the personal data has been disclosed, unless this would be impossible or would involve disproportionate effort. This communication will inform the third party of the rectification of the personal data.

19.10 Communication with the requestor

The Data Protection Officer will communicate with the requestor via letter or email to inform them whether their request has been followed and, if not, the reasons why. The Data Protection Officer will then update the tracker.

20.0 Right to Restriction of Processing Policy & Procedure

20.1 Right to restrict processing

A person shall have the right to restrict Incommunities/Sadeh Lok from processing that person's personal data in the following circumstances:

- the person is contesting the accuracy of personal data and the restriction is to allow time for the accuracy to be verified
- the processing is unlawful but the person asks for restriction of processing rather than erasure
- Incommunities/Sadeh Lok no longer needs the personal data but the person it for brining or defending a legal claim
- the person has object to processing under Article 21 and the restriction is to allow time to verify whether overriding interests apply to allow Incommunities/Sadeh Lok to continue processing

The exercise of this right is subject to the Restrictions section of this policy.

20.2 Recognising a right to restriction of processing request

These will usually be fairly obvious as they will expressly state that they want the processing to stop. If a recipient receives a request, or is unsure if a communication is such a request, it must be referred to the Data Protection Helpdesk as soon as reasonable practicable.

20.3 Responsibility

It is the responsibility of the recipient to forward the request to the Data Protection Helpdesk as soon as reasonably practicable. Once the request is received at the Data Protection Helpdesk, it is the Data Protection Officer's responsibility to handle the request. It is the responsibility of all staff members to assist the Data Protection Officer in handling such request.

20.4 Sufficiency of the request

A request must be sufficiently clear to enable the decision on whether to restrict processing the personal data to be handled. If it is not sufficiently clear, the recipient should seek clarification as soon as practicable. The time limit does not start running until a sufficiently clear request has been received.

20.5 Proving identity

Often, the recipient of a request to restrict processing will be sure of the identity of the requestor i.e. they will receive the request from a recognised email address, or the request will ask the response to be sent by post to a recognised home address. Where the recipient has doubts over the identity of the requestor, they should seek adequate proof. This may be as simple as asking the requestor to clarify their name, date of birth, home address etc., or it may require the requestor to provide identification such as photo ID (driving licence, passport) and a recently utility bill showing their address. The time limit does not start running until the requestor's identity is certain to the recipient.

20.6 Time limits

Generally, requests to restrict processing should be concluded within one calendar month of receipt. The Data Protection Officer manages a tracker which monitors this. It is the responsibility of the Data Protection Officer to ensure the time limit is met. If the request is particularly complex, the time limit can be extended by up to two further months but this should only be done with the Data Protection Officer's authorisation because it may need to be justified to the Information Commissioner in the event of a complaint by the requestor. The requestor must also be informed in writing of the extension and the reason for it.

20.7 Fees

No fees can be charged to fulfil a request to restrict processing, subject to the provisions on manifestly unfounded or excessive requests.

20.8 Manifestly unfounded or excessive requests

On occasion, requests to restrict processing are manifestly unfounded or excessive. If this is suspected, the Data Protection Officer will determine whether Incommunities/Sadeh Lok regards the particular request as manifestly unfounded or excessive. If such a determination is made, the Data Protection Officer will decide whether to charge a reasonable fee (the rule of thumb is £250 to cover the labour costs and administration costs of fulfilling the request) or to refuse the request.

20.9 Communication with third parties to whom the personal data has been disclosed

If the request is to be followed, the Data Protection Officer will communicate via letter or email with any recipient to whom the personal data has been disclosed, unless this would be impossible or would involve disproportionate effort. This communication will inform the third party of the restriction of processing.

20.10 Communication with the requestor

The Data Protection Officer will communicate with the requestor via letter or email to inform them whether their request has been followed and, if not, the reasons why. The Data Protection Officer will then update the tracker.