Policy

Data Protection

Responsible Officer:	Director of Legal & Governance
Approved:	June 2021
Review Date:	June 2024
Regulatory Standard:	Governance & Viability
Version:	4

Contents:

Introduction

Incommunities uses information as a tool as part of its business. We comply with our legal and regulatory obligations under the UK 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. However, if there is another lawful gateway that applies then this should be used in place of consent and an appropriate privacy notice should be issued.

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 asks staff, on a voluntary basis, for details of the sexual orientation to monitor 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 DPO or their deputy as soon as possible.

2.0 Incommunities Responsibilities and the Responsibilities of Joint Controllers and Processors

2.1 Incommunities Responsibilities

Incommunities recognises its responsibilities as a data controller. Incommunities 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 are reported more regularly and in more detail to the Board and Committees within the governance structure.

2.2 Joint controllers' responsibilities

When working with a partner as joint controllers of Personal Data an appropriate Data Sharing Agreement will be implemented, and the contract of engagement will set out the legal responsibilities each party bears as joint controller.

2.3 Processors' responsibilities

When working with a partner who is processing Personal Data on behalf of Incommunities an appropriate Data Sharing Agreement will be implemented, and the contract of engagement will set out the legal responsibilities each party bears as data controller and data processor.

3.0 The Consequences of Breaching Data Protection Obligations for Incommunities, their Staff and their Contractors

3.1 Consequences for Incommunities

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

- a complaint being made against Incommunities 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 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 £17.5 million or 4% of annual global turnover
- 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 may, if they have breached data protection laws (whether relating to their contract with Incommunities or otherwise) or Incommunities 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 or their deputy will then handle the matter.

4.0 Data Protection Officer (DPO)

4.1 A Data Protection Officer (DPO) shall be appointed by Incommunities Ltd. The appointee will be the DPO for Incommunities 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 in line with the DPA process and only where matters need to be escalated from the DP Manager.

- 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 their deputy and the Data Protection Manager, or appropriately trained staff and/or external contractors. These staff 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 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.

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 DPIA
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 DPIA outcomes
6. integrate the outcomes into the project plan
7. consult with internal and external stakeholders as needed throughout the process

All Projects undertaken by Incommunities must comply with the DPIA procedure and complete the screening questionnaire to determine if a full DPIA is required.

If this outcome is negative the screening questionnaire must be kept with project documents.

Id positive, a DPIA should be started as soon as possible, and consultation with the Date Protection Manager be ongoing as per the DPIA process. They can be contacted via DataProtection.Helpdesk@incommunities.co.uk. The DP Manager will sign off all DPIAs and save a copy. The commissioning directorate should also retain a copy of the DPIA. Disputes in sign-off will be dealt with in line with the agreed procedure.

Where a DPIA indicates that personal data processing would result in a high risk (in the absence of measures taken by Incommunities to mitigate that risk), The DPO or their deputy will inform the Information Commissioner in a manner that fulfils the requirements of Article 36(3) of the GDPR.

The DPIA procedure is attached at Appendix 2 of this policy. The accompanying template and triage questions are attached at Appendix 3 & 4 of this Policy.

6.0 Personal Data Security

6.1 Incommunities 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 risk appetite relating to personal data security.

6.2 Incommunities 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 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 Data Protection Officer, assisted by the Data Protection Manager/Deputy DPO has overall responsibility for Incommunities 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 policies, and reasonable requests from more senior employees, in order to maintain personal data security.

7.0 Retention Policy

7.1 Introduction

7.1.1 Retention of documents for an appropriate period 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 UK 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 will be personal data. The key requirements of Article 5 of the UK 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 policy on document retention; all staff are expected to abide by this guidance
- complement Incommunities 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 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 1: these set out the mandatory or recommended retention periods for the all the categories of document likely to be encountered within Incommunities.

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 and seek the assistance of the Data Protection Champion, 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 Data Protection Manager who can advise on minimum retention periods and whether a claim has been intimated which may require documents to be retained.

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 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 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 files 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 file falls outside the retention period and should be removed. This process can be undertaken on a periodic basis.

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
- confidential and/or work-related documents must only be disposed of on site at Incommunities offices. It should not be disposed of remotely.
- 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 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.

9.0 Monitoring Employees Policy & Procedure

9.1 Incommunities 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

9.2 Monitoring employees affects their privacy but can be undertaken if justified. Incommunities 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 https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

10.0 Data Protection Breach Management Policy

10.1 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

The breach procedure is attached at Appendix 5 of this policy and sets of the full details and roles in managing a data breach.

The accompanying documents for completion are attached at Appendix 6 & 7 of this Policy

10.2 Containment and recovery

The DPO or their deputy will lead the investigation; however, the requested assistance of any member of staff is compulsory.
However, immediately on discovery of a breach the relevant staff member must take immediate remedial action to contain and limit a breach. This is not an investigation but limiting the impact of the breach only.

The DPO or their deputy 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, instigate 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.

10.3 Assessment of ongoing risk

The DPO or their deputy will assess the ongoing risk by considering all of the circumstances. The risk assessment matrix, which is an appendix to the breach procedure, will be used to assess risk consistently.

10.4 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 in line with the appropriate assessment of risk using the risk assessment matrix.

The breach notification to the ICO will inform them of all relevant information to the breach, as logged on the risk matrix and any other relevant information requested.

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 DPO or their deputy 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).

10.5 Evaluation and response

The DPO or their deputy will evaluate the causes of the data protection breach, the circumstances leading to its discovery and how the breach was handled under the Incommunities breach 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.

10.6 Record-keeping

The DPO or their deputy 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.

11.0 Data Protection Training Policy

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

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

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

11.4 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.

12.0 Subject Access Requests Policy

12.1 Rights

The UK 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.

12.2 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.

12.3 Responsibility

The member of staff in receipt of a SAR will follow the SAR procedure for logging the SAR, which will ensure that the DP Manager and the directorate SAR co-ordinator are made aware of the SAR.
The SAR coordinator will ensure all papers required to fulfil the SAR as provided to the DP Manager within 7 working days, redacted and watermarked as per the procedure.

The DP Manager will send the SAR to the requestor.

12.4 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 SAR Coordinator, acting with the support of the DP Manager should seek clarification as soon as practicable. The time limit does not start running until a sufficiently clear request has been received.

12.5 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 SAR coordinator. The DP Manager will assist with ensuring there is adequate identification in place.

12.6 Time limits

Generally, subject access requests should be concluded within one calendar month of receipt. The DPO and their deputy manages a tracker which monitors this. It is the responsibility of the SAR Coordinator 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 DPO or their deputy’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.

12.7 Fees

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

12.8 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 or their deputy will determine in conjunction with the SAR coordinator whether Incommunities regards the particular subject access request as manifestly unfounded or excessive. If such a determination is made, the DPO or their deputy 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.

12.9 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.). Redactions will be made using adobe pro and all papers will be watermarked to indicate they were released subject to subject access request.

12.10 Concluding a subject access request

The data to be disclosed, properly redacted and watermarked will be sent, within 7 working days of the request arriving with the SAR coordinator to the DP Helpdesk. The DP Manager will review the papers, the redaction schedule if relevant and will send the final letter to the requestor. They will update the SAR tracker as appropriate. The DP Manager will retain a copy of the papers disclosed in line with the retention policy.

More detail on this is found in Appendix 8 which is the Subject Access Request Procedure.

13.0 Right to be Forgotten Policy & Procedure

13.1 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, 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.

13.2 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.

13.3 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 DPO or their deputy's responsibility to handle the request. It is the responsibility of all staff members to assist the DPO or their deputy in handling such request.

13.4 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.

13.5 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. The DP Manager can assist with issues around appropriate identification

13.6 Time limits

Generally, requests to be forgotten should be concluded within one calendar month of receipt. The DPO or their deputy manages a tracker which monitors this. It is the responsibility of the DPO and their deputy 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 DPO or their deputy'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.

13.7 Fees

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

13.8 Manifestly unfounded or excessive requests

On occasion, requests to be forgotten are manifestly unfounded or excessive. If this is suspected, the DPO or their deputy will determine whether Incommunities regards the particular request as manifestly unfounded or excessive. If such a determination is made, the DPO or their deputy 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. It is anticipated that such fees will rarely be applied.

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

If the request is to be followed, the Data Protection Officer or their deputy 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.

13.10 Communication with the requestor

The DPO or their deputy 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 DPO or their deputy will then update the tracker.

14.0 Right to Data Portability Policy & Procedure

14.1 Right to receive personal data

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

14.2 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.

14.3 Transmitting data

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

14.4 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.

14.5 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.

14.6 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 DPO or their deputy's responsibility to handle the request. It is the responsibility of all staff members to assist the DPO or their deputy in handling such request.

14.7 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.

14.8 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 recent utility bill showing their address. The time limit does not start running until the requestor's identity is certain to the recipient.

14.9 Time limits

Generally, requests should be concluded within one calendar month of receipt. The DPO or their deputy manages a tracker which monitors this. It is the responsibility of the DPO or their deputy 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 DPO or their deputy'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.

14.10 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 DPO or their deputy will determine whether Incommunities regards the particular request as manifestly unfounded or excessive. If such a determination is made, the DPO or their deputy 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. It is anticipated that such fees will rarely be applied

14.11 Communication with the requestor

The DPO or their deputy 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 DPO or their deputy will then update the tracker.

15.0 Right to Object Policy & Procedure

15.1 Right to object

A person shall have the right to object to Incommunities 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); or
- if Incommunities is processing the personal data for direct marketing.

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

15.2 Recognising a right to object request

These requests will 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.

15.3 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 or their deputy responsibility to handle the request. It is the responsibility of all staff members to assist the DPO or their deputy 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 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

15.4 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.

15.5 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.

15.6 Time limits

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

15.7 Fees

No fees can be charged.

15.8 Manifestly unfounded or excessive requests

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

15.9 Communication with the requestor

The DPO or their deputy 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 DPO or their deputy will then update the tracker.

16.0 Right to Rectification Policy & Procedure

16.1 Right to rectification

A person has the right to have their inaccurate personal data held by Incommunities 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.

16.2 Recognising a right to rectification request

These requests will 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.

16.3 Responsibility

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

16.4 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.

16.5 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.

16.6 Time limits

Generally, requests to rectify personal should be concluded within one calendar month of receipt. The DPO or their deputy manages a tracker which monitors this. It is the responsibility of the DPO or their deputy 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 DPO's or their deputies 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 rectify personal data, subject to the provisions on manifestly unfounded or excessive requests.

16.8 Manifestly unfounded or excessive requests

On occasion, requests to rectify personal data are manifestly unfounded or excessive. If this is suspected, the DPO or their deputy will determine whether Incommunities regards the particular request as manifestly unfounded or excessive. If such a determination is made, the DPO or their deputy 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. It is anticipated that such fees will rarely be applied.

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

If the request is to be followed, the DPO or their deputy 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.

16.10 Communication with the requestor

The DPO or their deputy 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 DPO or their deputy will then update the tracker.

17.0 Right to Restriction of Processing Policy & Procedure

17.1 Right to restrict processing

A person shall have the right to restrict Incommunities 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
- Incommunities no longer needs the personal data but the person it for bringing 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 to continue processing

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

17.2 Recognising a right to restriction of processing request

These requests will state that they want the processing being undertaken by Incommunities 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.

17.3 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 DPO or their deputy's responsibility to handle the request. It

is the responsibility of all staff members to assist the DPO or their deputy in handling such request.

17.4 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.

17.5 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.

17.6 Time limits

Generally, requests to restrict processing should be concluded within one calendar month of receipt. The DPO or their deputy manages a tracker which monitors this. It is the responsibility of the DPO or their deputy 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 DPO or their deputy'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.

17.7 Fees

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

17.8 Manifestly unfounded or excessive requests

On occasion, requests to restrict processing are manifestly unfounded or excessive. If this is suspected, the DPO or their deputy will determine whether Incommunities regards the particular request as manifestly unfounded or excessive. If such a determination is made, the DPO or their deputy 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. It is anticipated such charges would be applied rarely.

17.9 Communication with the requestor

The DPO or their deputy 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 DPO or their deputy will then update the tracker.

18.0 Related Documents & Appendix

1. Data Retention Schedule
2. Data Protection Impact Assessment Procedure
3. Data Protection Impact Assessment Template
4. Data Protection Impact Assessment Triage Questions
5. Incommunites Breach Procedure
6. Breach Scoring Matrix
7. Breach Reporting Template
8. Incommunites Subject Access Request Procedure