

**Data Protection Policy**

1. Scope and Aims of the policy
2. Equality and Diversity
3. Policy Statement
4. Disclosure of Data
5. Responsibilities
6. Data Protection Principles
7. Data Processing purposes
8. Data minimisation
9. Data Quality
10. Data Retention
11. Compliance Monitoring
12. Information Security
13. Data subject rights
14. Consent
15. Data Transfers and sharing
16. Information Asset Register
17. Risk Management
18. Personal Data Breaches
19. Data Processors
20. Monitor and Review
21. Relevant Legislation and Guidance
22. Relevant Hexagon policies and procedures

|  |  |
| --- | --- |
| Version | *Final* |
| Prepared by | *Policy officer* |
| Approved by | *Board/Committee/Directors Group* |
| Approved date | *21 July 2022* |
| Date of last review | *July 2022* |
| Document Owner | *Director of Housing Services* |
| Date of Next Review | *July 2024* |
| Lines of Defence/how is the document audited? | 1. *DHS will audit regularly – through spot checks*
2. *Internal DP Group*
3. *On Internal Audit programme*
 |

1. **Scope and Aims of the policy**
	1. The UK GDPR applies to any UK organisation involved in the processing (the use of data - collecting, storing, recording, consulting, altering, disclosing, erasing, making available) and filing of data by either automated or non-automated means.
	2. This policy applies to anybody who processes personal data for, or on behalf of, Hexagon and any external organisation or individuals with whom Hexagon shares or discloses personal data
	3. The policy will ensure compliance with all data protection legislation.
	4. Hexagon’s commitment to the protection of personal data, and the rights of those whose data it holds, will be ensured through upholding this policy.
2. **Equality and Diversity**
	1. An equality impact assessment ‘initial screening’ has been carried out which determined there to be a potentially positive impact regarding individuals’ protected characteristics.
	2. Data held about any of the protected characteristics must have a demonstrable purpose and should only be used to monitor and improve the service. This policy will clarify the way in which this data should be used and how we will oversee this.
3. **Policy Statement**
	1. Hexagon is committed to protecting the rights and freedoms of data subjects (any living individual who we have data for) whose information is collected and processed.
	2. The policy will apply to all Hexagon’s personal data processing functions, including those performed on personal data from residents, clients, employees, suppliers, contractors and partners, as well as any other sources.
	3. This policy will be reviewed periodically and in light of changes to the Information Asset Register, following managerial review or requirements stemming from Data Protection Impact Assessments.
	4. Partners, processors and any third parties working with Hexagon are expected to have read, understood and comply with this policy.
	5. No processor is authorised to process personal data on behalf of Hexagon without having first entered into a contract, which imposes obligations no less onerous than those to which Hexagon are committed and which gives Hexagon the right to audit as well as undertake other suitable data protection checks.
4. **Disclosure of Data**
	1. Hexagon ensures that personal data is not disclosed to unauthorised third parties (this includes family members, friends, government bodies and in certain circumstances the police). All employees must exercise caution when asked to disclose personal data to a third party and will receive training to deal with this risk.
	2. Hexagon does not share or disclose any personal data with any other controller, organisation or individual anyone who determines the purposes and means of processing personal data.) without having first entered in a Data Sharing Agreement and where a legal basis has been established.
	3. All requests to disclose personal data are governed by appropriate procedures and disclosures are authorised by the Data Privacy Officer. All data sharing activities are documented in the Register of Data Sharing Agreements.
5. **Responsibilities**

* 1. ***An internal information governance group*** oversees the implementation of UKGDPR of this policy and related procedures. The group meets quarterly.
	2. ***The Data Privacy Officer (DPO)*** . The DPO will be ultimately responsible for the monitoring of personal data within Hexagon and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This function is currently fulfilled by a specialist Consultant.
	3. ***The DPO and the Director of Housing Services*** and those in executive, managerial and supervisory roles within Hexagon are responsible for the developing good information handling practices, security aspects and arranging training within the organisation.
	4. The DPO and the Director of Housing Services has day-to-day responsibility for ensuring ongoing compliance with the data protection policy and legislation. Executives and managers also must ensure compliance in their areas of responsibility.
	5. The DPO Consultant will take responsibility for the procedures associated with data protection and be available to any employees with queries regarding data protection. The DPO monitors and reports to the Director of Housing Services in respect of compliance with the manual, arrange for the investigation of any security incidents, and maintain suitable records of processing activities. The Privacy Officer shall monitor the evolution of the Data Protection Legislation, case law, guidance, and codes of practice and incorporate relevant changes into the Organisation’s policy in a change-controlled manner.
	6. ***Information Asset Owner*** *–* Information Asset Owners are senior employees within each department who have been given direct responsibility for applying data protection principles over a particular process, contract or service. Their role is to understand:
* assess privacy risks to their information and protect them accordingly
* what information is held;
* what is added and what is removed;
* what information is moved;
* how long it should be kept for;
* who has access and for what purpose.
	1. ***The Human Resources team*** at Hexagon will provide appropriate training to assist employees in complying with data protection legislation.
	2. ***Hexagon employees*** are responsible for ensuring that any personal data about them and supplied by them to Hexagon are accurate and up-to-date.
1. **Data Protection Principles**
	1. Hexagon processes personal data in accordance with the principles defined in the UK GDPR and its data protection policy is designed to ensure these principles are adhered to. Hexagon processes personal data in a fair, lawful and transparent manner
	2. ***Fairness*** – no data collection activities are undertaken or commissioned without an appropriate privacy notice being provided to the data subject. A privacy notice will also be supplied to the data subject whose data is being processed if personal data is being collected from sources other than the subject. All privacy information and any changes to privacy information must be guided or approved by the relevant Information Asset Owner or the DPO.
	3. ***Lawfulness*** – no data collection activities are undertaken or commissioned without there being a lawful ground. The Information Asset Owner (IAO) determines the lawful grounds for processing and advises on lawful processing conditions. The lawful grounds will either be consent or legitimate interest; the appropriate procedure will be followed for either ground. The Information Asset Owner ensures there are grounds for all data processing activities that fall under their sphere of control and that the procedure for either gaining consent or establishing a legitimate interest has been followed. If Special Category Personal Data or data relating to a criminal offence is being processed, Hexagon will to establish the legal basis under Schedule One of the Data Protection Act.
	4. ***Transparency*** – Hexagon provides sufficient information about how personal data is being processed to enable transparency about its handling. The DPO periodically reviews transparency.
2. **Data Processing Purposes**

7.1 Data obtained for specific purposes is not used for any reason other than that purpose.

1. **Data Minimisation**
	1. Hexagon uses a minimum of personal data in its processing activities and periodically reviews the relevancy of the information that it collects. Information Asset Owners ensure that no unnecessary, irrelevant or unjustifiable personal data are collected or created (directly or indirectly) through the data processing activities they are responsible for. The DPO advises on justifiable data held.
	2. The IAO ensures that Hexagon does not collect information that is not strictly necessary for the purpose it was obtained.
	3. All data collections forms include a fair processing statement or link to privacy information and are guided and approved by the DPO
	4. The IAO ensures that, on an annual basis, all data collection methods are reviewed by an internal information governance group, to ensure that personal data collected continues to be adequate, relevant and not excessive. The DPO/Director of Housing Services will conduct periodic spot checks.
2. **Data Quality**
	1. Hexagon recognises that the accuracy of data is important, and that some data is more important to keep up-to-date than others. Hexagon will take reasonable steps to ensure information is as accurate and current as possible (particularly where out of date or inaccurate data will have a detrimental impact on data subjects). Information Asset Owners ensure that personal data created either directly or indirectly through their processing activities are accurate and up-to-date. Any data that cannot reasonably be assumed to be accurate should either be erased or anonymised. The DPO can advise on data accuracy.
	2. Personal data is maintained, accurate and up-to-date with every effort made to erase or rectify obsolete personal data without delay.
	3. Personal data stored by Hexagon is reviewed and updated, as necessary. No data is kept unless it is reasonable to assume it is accurate.
	4. The DPO and IAO ensure that all employees are trained in the importance of collecting accurate data and maintaining it.
	5. Data subjects are expected to ensure that their personal data, held by Hexagon, is accurate and up-to-date. Completion of a registration or application form by a data subject includes a statement that the data contained therein is accurate at the date of submission.
	6. Residents, customers, suppliers, employees and others are expected to notify Hexagon of any changes in circumstance to enable personal data to be updated accordingly. Hexagon will ensure any notification received regarding changes to personal data is recorded and actioned.
	7. The DPO, with the collaboration of the Policy Officer, ensures that policies and procedures regarding information governance are in place, taking into account the volume of data collected, the speed it may change and other relevant factors.
	8. Each IAO responds to requests for rectification from data subjects within one calendar month. This can be extended to a further two months for complex requests. If Hexagon decides not to comply with the request, the relevant IAO responds to the subjected to explain the reasoning and informs the subject of their right to complain to the supervisory authority and seek judicial remedy.
	9. The IAO makes appropriate arrangements to inform processors or controllers if they have been supplied with incorrect or out-of-date personal data. They will be told the inaccurate data is not to used and any corrections will be supplied where possible.
3. **Data Retention**
	1. Hexagon ensures that it does not retain personal data for any longer that is necessary for the purposes for which it was collected. Appropriate measures, such as erasure or anonymisation, will be applied when the data is at the end of its useful life.
	2. Hexagon may store data for longer periods if the personal data is processed solely for archiving purposes in the public interest, for research, or for statistical purposes. This is subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of data subjects. In order to extend the life of data beyond its retention period, Hexagon will seek a lawful basis to do so including renewed consent The DPO must review and approve this,
	3. Information Asset Owners determine the retention period for personal data under their control.
	4. The Data Privacy Officer (DPO) maintains a schedule of data retention periods in the Data Retention Schedule which defines approved retention periods and end of life treatment. The Data Retention Schedule defines the reasoning for data retention periods. These may be influenced by different factors, including: statutory, regulatory, financial, industry sector best-practice or business considerations.

The IAO approves all retention periods for personal data. Retention periods for all information assets are made publicly known to the data subjects. Any changes to retention periods and/ or information assets results in an update to the published versions. The Data Retention Schedule should be made available to data subjects on request.

* 1. Retention and end-of-life of Personal Data Procedure.
	2. Personal data that has exceeded its retention period will be deleted, given a pseudonym or destroyed, as defined in the Data Retention Schedule. Personal data that has exceeded its retention period but is the subject of a Data Subject Rights request, an investigation by the supervisory authority or legal proceedings will be retained until that request, investigation or proceeding is concluded. The DPO will advise in such a situation.
	3. Personal data is disposed of securely in accordance with the principles of UK GDPR – processed in an appropriate manner to maintain security, thereby protecting the “rights and freedoms” of data subjects.
1. **Compliance Monitoring**
	1. Hexagon ensures compliance with this policy by monitoring and auditing to ensure that personal data is managed, retained and disposed of in compliance with the Data Retention Schedule.
	2. All retention periods (including any that are defined as indefinite retention) are reviewed annually and updated as appropriate under the guidance of the Information Asset Owner and the DPO.
2. **Information Security**
	1. Hexagon ensures the appropriate security for any personal data that it processes (or commissions the processing of). This means taking appropriate technical or organisational measures to protect against threats including unauthorised or unlawful processing, accidental loss, destruction or damage. The IT Manager, with advice from the DPO as necessary, will ensure an Information Security Management Policy is maintained which sets out how data will be maintained securely, confidentially and in a way that is available.
	2. Data Protection Impact Assessments are conducted as appropriate, taking into account all the circumstances of Hexagon’s controlling or processing operations.
	3. In determining appropriateness, the IAO considers the extent of possible damage or loss that be caused to the data subjects if a personal data breach a breach of security or control leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed occurs the effect of a breach on Hexagon, and any likely reputational damage (including the possible loss of customer trust).
	4. Information security controls are selected based on identified risks to personal data, and the potential for damage or distress to data subjects whose data is being processes (as documented in the Risk Register).
	5. Hexagon complies with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, a Data Protection Impact Assessment Procedure, a Data Protection Breach procedure and incident response plans.
	6. All employees ensure that any personal data that Hexagon holds, and for which they are responsible, is kept securely and is not under any condition disclosed to any third party without specific authorisation by the DPO and a data sharing agreement.
	7. All personal data is accessible only to those who need to use it. All personal data is treated with the highest security and is kept:
* In a lockable room with controlled access; and/ or
* In a locked drawer or filing cabinet;
* If digital, password protected;
	1. Care is taken to ensure that Personal Computer screens are not visible except to authorised employees of Hexagon. All employees enter into an Acceptable Use Agreement before they are given access to organisational information of any sort.
	2. Paper records are not left where they can be accessed by unauthorised personnel and are not removed from any working environment without explicit written authorisation by their line manager. As soon as paper records are no longer required for the defined purposes, they are removed from secure archiving.
	3. Personal data is deleted or disposed of in line with agreed schedules and this policy. Paper records that have reached their retention date are shredded and disposed of as ‘confidential waste’. Hard drives of redundant PCs are removed and destroyed before disposal.
	4. Processing of personal data ‘off-site’ presents a greater risk of loss, theft or damage. Employees do not process data off-site, unless specifically authorised by their manager.
1. **Data Subjects’ Rights**
	1. Hexagon recognises the legal rights of the data subjects whose personal data it is processing (or intends to process) and ensures that appropriate information is provided to advise them of their rights. Hexagon’s policies and procedures, namely the Data Subject Rights Procedure, are maintained to ensure Data Subject Rights requests are recognised. Data subjects have the following rights regarding data processing, and the personal data that is recorded about them:
	* To make Data Subject Access Requests regarding the nature of information held about them and to whom it has been disclosed;
	* To prevent processing likely to cause damage or distress;
	* To object to processing for purposes of direct marketing;
	* To be informed about the mechanics of automated decision-making processes that will significantly affect them;
	* To not have significant decisions that will affect them taken solely by an automated process;
	* To seek compensation if they suffer damage by any contravention of the UK GDPR;
	* To take action to rectify, block, erase, or destroy inaccurate data, including the right to be forgotten;
	* To lodge a complaint with the Information Commissioners Office ;
	* To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller;
	* To object to any automated profiling that is occurring without consent.
	1. Data subjects may exercise their rights through any method including, but not limited to:
* In writing;
* Over the phone;
* Through social media;
* By letter.
1. **Consent**
	1. Hexagon understands ‘consent’ to mean a specific, informed and unambiguous indication of the data subject’s wishes, given explicitly and freely. This is supplied by clear affirmative action signifying agreement to the processing of personal data relating to the subject. Consent can be withdrawn at any time.

14.2 Consent means the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information is not a valid basis for processing.

* 1. Hexagon ensures that there is active communication with the data subject to demonstrate active consent. Consent is not inferred from non-response to a communication. Hexagon demonstrates that consent was obtained for the processing operation.
	2. All employees must use the approved Consent form for when obtaining and recording consent; this must be in writing in order to evidence consent. There may be limited circumstances where consent can be obtained verbally either in person or over the phone, where this is the case, employees are required to record when (time/date) and what consent was obtained for, by whom, and who was consented to discuss on behalf of the customer.
	3. For special categories of personal data explicit written consent of data subjects is obtained unless an alternative lawful basis for processing exists.
	4. In most instances, consent to personal data (and when appropriate, special categories of data) is obtained routinely by Hexagon using standard consent documents (e.g. when a new tenant signs a tenancy agreement or during inductions for participants on a programme). These will be refreshed when reasonable.
	5. Hexagon will have a lawful basis for processing a child’s personal data. Consent is one possible lawful basis for processing, but it is not the only option.
	6. Where Hexagon provides online services to children, only children aged 13 or over are able to provide their own consent and we will get it. For those children under 13, we will get consent from whoever holds parental responsibility for the child.
	7. As a matter of good practice, we use DPIAs to help us assess and mitigate the risks to children.
1. **Data Transfers and Sharing**
	1. Data sharing can take the form of:
* A reciprocal exchange of data;
* One or more controllers providing data to a third party or parties e.g. sharing CCTV images to assist with a criminal investigation;
* Several organisations pooling information and making it available to each other;
* Organisations pooling information and making it available to a third party or parties (e.g. anti-money laundering authorities);
* Exceptional, one-off disclosures of data in unexpected or emergency situation.
	1. When Hexagon is obliged to share personal data for legal or regulatory reasons, it still informs data subjects accordingly unless an exception applies under Data Protection Legislation. The principal method of communicating this is via the Privacy Policy. This will apply unless sharing is required by law.
	2. Any systematic or routine sharing of data between Hexagon and another party on a controller-to-controller basis is defined and detailed in a Data Sharing Agreement before any data sharing commences. This will apply unless sharing is required by law.
	3. Such Data Sharing Agreements articulate the roles of the data controllers and in particular avoid any circumstances where one of the parties could otherwise be construed as a processor, rather than a controller. The agreements are filed centrally and documented in the Register of Data Sharing Agreements.
	4. Hexagon only enters into data sharing activities where it is proven and documented that the data sharing is fair and lawful.
	5. Hexagon only shares personal data for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes.
	6. Hexagon only shares personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
	7. Sharing personal data with an unauthorised controller or sharing data in the absence of a valid Data Sharing Agreement is deemed to be a data breach and is investigated by the Data Privacy Officer/Data Protection team and Information Asset Owner (IAO) in accordance with the Breach Reporting Procedure.
	8. Any breach of this policy is dealt with under Hexagon’s disciplinary policy and if it is also a criminal offence, the matter is reported as soon as possible to the appropriate authorities.
	9. When Hexagon receives a Data Subject Rights request, such as a request to correct inaccurate personal data, Hexagon informs any other controller with whom the data has be shared.
	10. When sharing information with another controller, Hexagon recognises this as a risk to the rights and freedoms of data subjects and records this in the Data Protection Risk Register.
	11. Exports of data from the UK are unlawful unless there is an appropriate level of protection for the fundamental rights of data subjects.
	12. Hexagon will ensure that any data transfer to a country outside the UK will have the appropriate safeguards or meet the criteria for an exception set out in the UK GDPR.
	13. Hexagon is legally obliged to share certain personal data for tax, criminal or other legal reasons.
	14. In these circumstances sharing information with the relevant authority is a mandatory requirement – Hexagon will cooperate fully and share the appropriate information (disclosure will be subject to the ad hoc sharing procedure defined below).
	15. No data can be shared internally and/or externally without confirming the recipient of the information, the purpose(s) of sharing the said information and, the lawful grounds for the sharing operation.
	16. This section functions in conjunction with the Data Sharing Procedure (controller-to-controller) to define how and when Hexagon shares personal data with another controller
1. **Information Asset Register**

16.1 Hexagon maintains an Information Asset Register and an analysis of data flows as part of its approach to address risks and opportunities involving personal data. Hexagon’s Information Asset Register and data flow analysis determines:

* + Business processes that use personal data;
	+ Source(s) of personal data;
	+ Volume of data subjects;
	+ Descriptions of each item of personal data;
	+ Processing activity;
	+ Maintains the inventory of data categories of personal data processed;
	+ Documents the purpose(s) for which each category of personal data is used;
	+ Recipients, and potential recipients, of the personal data;
	+ The role of Hexagon throughout the data flow;
	+ Key systems and repositories;
	+ Any data transfers; and
	+ All retention and disposal requirements
1. **Risk Management**
	1. Hexagon assesses the level of risk to data subjects associated with processing their personal data. Data Protection Impact Assessments are conducted in relation to Hexagon’s processing activity and for processing done on Hexagon’s behalf.
	2. Hexagon manages any risks identified by the risk assessment to ensure compliance with data protection standards.
	3. Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, Hexagon conducts a Data Protection Impact Assessment prior to processing. A single Data Protection Impact Assessment may address a set of similar processing operations with similar risks.
	4. Where, as a result of a Data Protection Impact Assessment, it is clear that Hexagon is about to commence processing of personal data that could damage and/ or distress data subjects, the decision on whether Hexagon will proceed will be reviewed by the both the DPO and IAO/Director of Housing Services
	5. When there are significant concerns, either potential damage or distress, or the quantity of data concerned, the DPO will escalate to the supervisory authority.
	6. Appropriate controls are selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Hexagon’s documented risk acceptance criteria and the requirements of the UK GDPR. This is recorded in the Data Protection Risk Register.
	7. The IAO are responsible for ensuring that all actions identified during a risks assessment or DPIA, is remediated accordingly and appropriately.
	8. All employees are required to undertake a risk assessment during the project planning stage and prior to changes in data processing operations or, introduction of new technologies or new projects. The DPIA screening questions will support employees with establishing whether a full DPIA is required.
2. **Personal Data Breaches**
	1. Hexagon will maintain a ***Breach Reporting Procedure*** and will ensure that all employees and those with access to personal data are aware of it and this personal data breaches policy.
	2. The [IAO]/[lead investigator] shall be responsible for maintaining the ***Breach Reporting Procedure*** and for ensuring that all relevant people are made aware of it.
3. **Data Processors**
	1. Hexagon reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness, ensuring that:
* There are satisfactory assurances that the processor will handle personal data in accordance with Data Protection Legislation.
* Appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment.
* A written agreement shall be implemented between the organisation and the data processor which at least meets the requirements of the Data Protection Legislation. The data processor agreement will specify what is to happen to personal data upon termination of the data processing agreement.
* No employee is permitted to commission or appoint a third party to process data on behalf of Hexagon without adhering to this policy.
* The DPO shall maintain operational instructions on the steps to take to appoint a data processor. Please see the Data Sharing procedure.
1. **Monitor and Review**
	1. Data compliance, collection methods, retention periods and impact assessments will be continuously reviewed by the [DPO]/[Policy Officer].
	2. Additionally, Hexagon will convene an internal group to periodically review these themes.
	3. The group will be comprised of representatives from different areas of the business with the specific purpose of reviewing data protection issues.
2. **Relevant Legislation and Guidance**
* Data Protection Act 2018 (DPA 2018)
* UK General Data Protection Regulation (UK GDPR).
1. **Related Hexagon policies and procedures**
* Data Breach Procedure 2021
* Data Subject Rights Procedure 2021
* Data Privacy Impact Assessment procedure 2021
* Data Sharing Procedure 2021
* Data retention procedure 2021