

|  |
| --- |
| **North Wales Housing** |
| **GDPR Data**  **Protection Policy** |

|  |  |
| --- | --- |
| **Owner** | Malcolm Wilson |
| **Directorate** | Resources - IT |
| **Approved by** | Board 29 March 2018 |
| **Next review date** | March 2020 |
|  |  |

|  |  |  |
| --- | --- | --- |
|  | **Contents** | **Page** |
| **1** | Introduction | 2 |
| **2** | Policy scope and objectives | 2 |
| **3** | Data protection principles | 4 |
| **4** | Data subjects’ rights | 8 |
| **5** | Consent | 9 |
| **6** | Responsibilities under the General Data Protection Regulation | 10 |
| **7** | Notification | 11 |
| **8** | Disclosure of data | 12 |
| **9** | Direct marketing | 13 |
| **10** | Employees | 14 |
| **11** | Suppliers and Contractors | 15 |
| **12** | Risk and Data Protection Impact Assessment | 15 |
| **13** | Security breaches | 16 |
| **14** | Records and Housekeeping | 16 |
| **15** | Training | 17 |
| **16** | Monitoring and reporting | 17 |
| **17** | Linked policies | 18 |
|  | **Appendix A – Glossary of Definitions** | 19 |

**North Wales Housing Association is committed to equality and diversity. This policy has considered the Equality Act 2010 and its protected characteristics which are: race, gender, gender reassignment, disability, religion or belief, sexual orientation, age, marriage, civil marriage and partnership, and pregnancy and maternity explicitly.**

**We will make sure that all of our communication is fully accessible and to achieve this if a policy or document needs to be available in other formats we will provide them.**

**1. Introduction**

1.1 The General Data Protection Regulation (GDPR) of 2016 will be effective from 25 May 2018 and completely replaces all previous Data Protection laws. Its purpose is to protect the “rights and freedoms” of living individuals, and to ensure that personal data is not processed without their knowledge and is processed with their consent.

1.2 GDPR introduces a number of new concepts and improvements of data subjects’ rights. A summary of the new regulations is given below:

* gaining explicit consent from data subjects for the use of their personal data;
* processing relevant and adequate personal information, only where this is strictly necessary for legitimate organisational purposes;
* collecting only the minimum personal information required for these purposes and not processing excessive personal information;
* providing clear information to individuals about how their personal information will be used and by whom;
* processing personal information fairly and lawfully;
* maintaining an inventory of the personal information categories that North Wales Housing Association (NWHA) processes;
* personal information is accurate and, where necessary, up to date;
* retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
* keeping all personal information secure;
* only transferring personal information outside the EU in circumstances where it can be adequately protected or where equivalent standards apply;
* the application of the various allowable exemptions;
* the requirement to appoint a Data Protection Officer (DPO) in some circumstances;
* ‘special categories’ of personal data (previously sensitive personal data) is extended to include biometric and genetic data;
* mandatory reporting of data breaches/loss;
* enhanced security of personal data, e.g. encryption and anonymisation;
* respecting subject’s access rights, including new provisions such as data portability.
* Making data subjects, i.e. individuals whose data we hold, aware of their rights before obtaining or processing any personal information

Appendix A provides a glossary of definitions

**2. Policy statement, scope and objectives**

NWHA is committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the “rights and freedoms” of individuals whose information NWHA collects and processes in accordance with the GDPR.

NWHA necessarily and routinely uses personal information when it carries out many aspects of its day to day business. The whole organisation is subject to the policy with some requirements spreading out and imposing responsibilities on partner organisations, e.g. our maintenance contractors. (Typically they are a Data Processor of personal data that we have collected in our role of Data Controller).

Personal data that is within the scope of GDPR is all data within our computer systems, including our Housing Management System, Document Management System, email, Word documents, Excel worksheets, plus manual structured filing systems, i.e. paper based. (A structured filing system is defined as having a form of index enabling fast and easy access to individual documents within it. A filing system in just date order, without any such index, would not be considered a structured system). To avoid any doubt the scope of GDPR also includes text messages, videos, photographs, post-it notes, note books, print outs and hand written letters etc.

The GDPR and this policy apply to:

* All of NWHA’s personal data processing functions, including those performed on customers’, clients’, employees’, suppliers’ and partners’ personal data and any other personal data the organisation processes from any source, including archived data both digital and paper.
* All employees of NWHA. Any breach of the GDPR (or this policy) will be dealt with under the disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

A Data Protection Officer (DPO) is in process of being appointed. The DPO is responsible for reviewing annually the register of processing in light of any changes to NWHA’s activities, management review or any additional requirements identified by means of Data Protection Impact Assessments. Such documentation may need to be available to the supervisory authority on request.

Partners and any third parties working with NWHA who may have access to personal data, will be expected to have read, understood and comply with the requirements and agreements in our Supplier DP Responsibilities policy. This policy imposes obligations on the third party that are no less onerous than those to which NWHA is committed, and gives us the right to audit compliance with the Supplier agreement.

The policy’s objectives are to:

* protect the personal data interests of individuals and other key stakeholders by the use of appropriate procedures and controls.
* provide the supporting framework for achieving and maintaining GDPR compliance.
* ensure NWHA meets applicable statutory, regulatory, contractual and/or professional duties.

**3. Data protection principles**

**3.1. Personal data must be processed lawfully, fairly and transparently.**

*Lawfully*

A lawful basis must be identified before personal data is processed. This are often referred to as the “conditions for processing”, e.g. consent.

*Fairly*

In order for processing to be fair, the Data Controller has to make certain information available to the data subjects if practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the ‘Transparency’ requirement.

*Transparently*

The GDPR includes rules on giving privacy information to data subjects set out in Articles 12, 13 and 14 of the regulations. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. (See NHWA’s Customer Privacy policy and Fair Processing Notice).

Specific information that must be provided to the data subject must, as a minimum, include:

* the identity and contact details of the controller and the controller's representative, if any;
* the contact details of the Data Protection Officer;
* the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
* the period for which the personal data will be stored;
* the existence of rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
* the categories of personal data concerned;
* the recipients or categories of recipients of the personal data, where applicable;
* where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
* any further information necessary to guarantee fair processing.

**3.2. Personal data can only be collected for specified, explicit and legitimate purposes.**

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of NHWA’s GDPR registration. NHWA’s registration reference is Z5865343 and details of the registration entry may be seen on the supervisory authority’s website. <https://ico.org.uk/ESDWebPages/Entry/Z5865343>

Where there is a change in purpose (other than the original purpose for which the data was collected), prior to further processing, we must provide the data subject with information on the new purpose.

**3.3. Personal data must be adequate, relevant and limited to what is necessary for processing.**

The DPO is responsible for ensuring that NWHA does not collect information that is not strictly necessary for the purpose for which it is obtained.

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and be approved by the DPO.

The DPO will ensure that, on a regular basis, all data collection methods are audited to ensure that collected data continues to be adequate, relevant and not excessive.

If data is given or obtained that is excessive or not specifically required by NHWA’s documented procedures, the DPO is responsible for ensuring that it is securely deleted or destroyed in line with the Document and Data Retention policy.

**3.4. Personal data must be accurate and kept up to date.**

Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.

Whilst our customers and staff should notify us of any changes in circumstance, regular proactive collection and checking campaigns will be necessary. It is the responsibility of NWHA to ensure that any notification regarding change of circumstances is noted and acted upon.

The DPO is responsible for ensuring that:

* At least annually the retention dates of all the personal data processed by NWHA are reviewed to identify any data no longer required and arranging secure deletion/destruction.
* We respond to requests for rectification from data subjects within one month. If NWHA decides not to comply with the request, the DPO must respond to the data subject to explain the reasoning and inform them of their right to complain.
* We make appropriate arrangements where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is not to be used to inform decisions about the individuals concerned and for passing on any corrections.

**3.5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.**

Where personal data is retained beyond the processing date, it should be ‘obfuscated’ by being minimised, encrypted or pseudonymised in order to protect the identity of the data subject. This is dependent on the technical capabilities available.

Personal data will be retained in line with our Document and Data Retention policy. Once its retention date is passed, it must be securely destroyed.

The DPO must specifically approve in writing any data retention that exceeds the retention periods and ensure that the justification is clearly identified in line with data protection legislation.

**3.6. Personal data must be processed in a manner that ensures the appropriate security.**

The DPO will carry out a risk assessment, taking into account all the circumstances of NHWA’s controlling or processing operations.

In determining appropriateness, the DPO will also consider the extent of possible damage or loss that might be caused to individuals if a security breach occurs; the effect of any security breach on NWHA; and any likely reputational damage, including the possible loss of customer trust.

When assessing appropriate technical measures, the DPO will consider the following:

* Password protection;
* Automatic locking of idle terminals;
* Removal of access rights for USB and other memory media;
* Virus checking software and firewalls;
* Role-based access rights including those assigned to temporary staff;
* Encryption of devices that leave the organisations premises such as laptops;
* Security of local and wide area networks;
* Privacy enhancing technologies such as pseudonymisation and anonymization;
* Identifying appropriate international security standards relevant to NWHA.

When assessing appropriate organisational measures the DPO will consider the following:

* The appropriate training levels throughout NWHA;
* Measures that consider the reliability of employees;
* The inclusion of data protection in employment contracts;
* Identification of disciplinary action measures for data breaches;
* Monitoring of staff for compliance with relevant security standards;
* Physical access controls to electronic and paper based records;
* Adoption of a clear desk policy;
* Storing of paper based data in lockable fire-proof cabinets;
* Appropriate controls on portable electronic devices outside of the workplace;
* Similar controls and checks on the use of employee’s own personal devices being used in the workplace (currently nothing is in place for bring your own devices);
* Adopting clear rules about passwords;
* Making regular backups of personal data and storing the media off-site.

These controls have been selected on the basis of identified risks to personal data and the potential for damage or distress to individuals whose data is being processed.

Personal data shall not be transferred to a country or territory outside the European Union unless it has an adequate level of protection for the ‘rights and freedoms’ of data subjects.

The GDPR goes to some length to describe the controls that must be in place for the transfer of data outside the European Union area and a number of new concepts are introduced. A brief description of safeguards and mechanisms is given in the separate procedure – Transfer of personal data outside the EU area.

**4. Data subjects’ rights**

**4.1 Data Processing**

Data subjects have the following rights regarding data processing and the data that is recorded about them:

* To make subject access requests regarding the nature of information held and to whom it has been disclosed. A number of exemptions apply whereby personal data does not have to be disclosed – see the Subject Access Request procedure.
* To prevent processing for purposes of direct marketing.
* To be informed about the mechanics of automated decision-taking process that will significantly affect them.
* Not to have significant decisions that will affect them taken solely by automated processes.
* To sue for compensation if they suffer damage by any contravention of the GDPR.
* To take action to rectify, block, erase or destroy inaccurate data including the right to be forgotten.
* To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
* 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.
* Where possible to halt processing of data while it is being queried or subject to a Subject Access Request

**4.2 Complaints**

Data subjects who wish to complain about how their personal information has been processed may:

* use the complaints procedure;
* complain directly to the DPO;
* complain to the supervisory authority.

**4.3 Rights of access to data**

Data subjects have the right to access any personal data held by NWHA in electronic format and manual records which form part of a structured filing system. This includes the right to inspect confidential personal references received by NWHA and information obtained from third-party organisations about that person.

Subject Access Requests are dealt with as described in the DP Subject Access Request Procedure.

**5. Consent**

NWHA understands ‘consent’ to mean that:

* it has been explicitly and freely given, being a specific, informed and unambiguous indication of the data subject’s wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.
* the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

Withdrawal of consent will affect how, or indeed if, we can deliver services to those customers. Data fields in appropriate systems will need to be changed to a ‘refused’ state.

There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances, consent to process personal and sensitive data is obtained routinely by NWHA using standard consent documents, e.g. when a new client signs a Tenancy Agreement.

Where NWHA provides online services to children (defined as being under the age of 16 the UK age of consent), parental or custodial authorisation must be obtained.

Under certain circumstances, NWHA may receive information about residents from partner agencies, especially the police or local authorities. Employees requiring advice on how to treat this information should discuss it with their manager or the DPO.

The lawful processing ‘gateway’ of being necessary for purposes of legitimate interests is now expressly unavailable to public authorities. Any legal obligation or task in the public interest must be laid down in EU or national law, which must itself be in the public interest and proportionate to the aim.

It is likely that the ‘consent is given by the resident’ lawful processing gateway that we have used historically will not meet the more stringent demands of GDPR. Therefore each gateway will be reviewed to ensure they are compliant.

Registered Providers are classed as Community Benefit Societies and are ’hybrid’ organisations, mid-way between the public and private sectors. In the absence of clear guidance (in the GDPR, by Working party interpretation or by the UK supervisory authority), they are taken to be in the private sector for GDPR purposes.

**6. Responsibilities under the General Data Protection Regulation**

**6.1 General responsibilities**

NWHA is a data controller and in some circumstances a data processor under the GDPR.

The Board has overall responsibility for ensuring good information handling practices and for reviewing and approving this policy.

Directors, managers and supervisors are responsible for developing and encouraging good information handling practices. Responsibilities are set out in role profiles.

Compliance with data protection legislation is the responsibility of all employees who control or process personal data.

Employees are responsible for ensuring that their own personal data is accurate and up to date.

Customers who will be providing personal data will need to be shown the Fair Processing Notice at an appropriate point.

**6.2 Data Protection Officer**

The DPO is accountable to the Senior Management Team for the management of personal data, and ensuring good practice and that compliance with legislation can be demonstrated. This includes:

* development and implementation of this policy
* security and risk management in relation to compliance with this policy.
* having data protection expertise
* undertaking an annual review of personal information held to ensure that there is a sound business reason for holding that information.

Directors and senior managers have equivalent responsibility and accountability for the control of personal data within their area of responsibility.

The DPO has specific responsibilities for designing procedures such as for Subject Access Requests. These will be handled by other staff but the DPO will provide staff with clarification on any aspect of data protection legislation and compliance.

**6.3 Policy Applicability**

Partners and any third parties working with NWHA who have access to personal information, will be expected to read, understand and comply with this policy. No third party may access personal data held by NWHA without having first entered into our Supplier Agreement. (This imposes security and data confidentiality obligations no less onerous than those to which NWHA is committed, and gives NWHA the right to audit compliance with the agreement).

This policy applies to all employees and any breach of the GDPR regulations or this policy will be dealt with under the Disciplinary policy. If there is a criminal offence; it may be reported to the appropriate authorities.

**6.4 Accountability**

The GDPR introduces the principle of accountability which states that the Data Controller is not only responsible for ensuring compliance but also for demonstrating that each processing operation complies with the GDPR. Specifically, Data Controllers are required to:

* maintain necessary documentation of all processing operations;
* implement appropriate security measures;
* perform Data Processing Impact Assessments (DPIAs);
* comply with requirements for prior notifications, or approval from supervisory authorities;
* appoint a DPO if required.

**7. Notification**

NWHA has notified the supervisory authority that it is a Data Controller and processes certain information about data subjects. NWHA has identified all the personal data that it processes and this is contained in the Personal Data and Purposes log.

A copy of the supervisory authority notification (the register entry) is retained and renewed annually by the DPO. Any changes to NHWA’s activities, (e.g. from DPIAs) are notified by the DPO.

One interpretation of the GDPR is that we will no longer have to register with the UK supervisory authority. Another indicates that we can supply fewer details, although internal records of processing activities will need to be enhanced. Full clarification on notification will be required before any change will be made to the registration details of NWHA.

**8. Disclosure of data**

**8.1 Exemptions**

The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

* to safeguard national security;
* prevention or detection of crime including the apprehension or prosecution of offenders;
* assessment or collection of tax duty;
* discharge of regulatory functions (including health, safety and welfare of persons at work);
* to prevent serious harm to a third party;
* to protect the vital interests of the individual, e.g. emergency medical situations.

All requests to provide data for one of these reasons must be supported by appropriate ‘justification’ paperwork and all such disclosures must be specifically authorised by the DPO.

This exemption allows the release for the stated purposes and does not cover the disclosure of all personal information in all circumstances. The following types of verification and limitation questions will be asked:

* Is the person requesting the information who they say they are?
* Is their intention to prevent or detect a crime, catch or prosecute an offender or assess or collect tax or duty?
* If the information is not released, will this significantly harm prevention of a crime or catching of a suspect? (The risk must be that the investigation may be impeded.)
* What is the minimum amount of information to enable them to do their job?
* What else needs to be known to be sure that the exemption applies?

**8.2 Information Sharing**

NWHA must ensure 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 should exercise caution when asked to disclose personal data held on an individual to a third-party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of NHWA’s business.

Information Sharing Agreements in place, e.g. with the police, councils and other agencies, using sharing protocols.

Board members do not have any right to see personal data stored on files, except with the written permission of the individual, or any information that would not be disclosed to the individual, except as is necessary in the course of their duties.

There are situations where information will be withheld, such as where it would identify someone else who has not given consent to the disclosure, unless it can be edited out (redaction). Joint tenants will be asked if they agree to their data being shared if only one makes the request, otherwise all of the references to the other joint tenant will have to be redacted. There may be other exemptions specifically relating to health information.

If there are concerns that the GDPR would be breached, a court order requiring the release will be requested and the DPO will advise.

**8.3 Safeguarding information**

NWHA actively works to safeguard children, young people and vulnerable adults from harm. NWHA has a duty to tell Social Services where an individual’s safety is at risk and share information with them, whether the concerns are identified by or directly reported to staff. The types of information that may be shared include names, contact details, information about a person’s physical or mental health and relations with others.

NWHA has detailed procedures that cover the reporting of this information which follow different local safeguarding information sharing protocols. NWHA expects its staff to immediately report any concerns the safeguarding lead who will report the information in accordance with the Safeguarding policy.

In certain limited circumstances the Act provides for personal data, even sensitive data, to be shared without the individual knowing about it.

**9. Direct marketing**

NWHA may use personal data for direct marketing (including to business partnerships) in relation to its activities. This includes email and text, phone calls and direct mailshots. Consent will be obtained at the time that personal data is provided by the individual. Any individual can exercise their right, at any time, to opt out of their personal data being used in this way and NWHA will accord with their request.

Our computer systems record the contact preferences of residents (if and how) and, of course, will be followed.

**10. Employees**

Personal data relating to employees is obtained from job applications and whenever data is refreshed through the HR department or Payroll. The job application form states that the information collected will be strictly confidential and used only for the purposes of personnel and salary administration, or otherwise in connection with NHWA’s business. This includes using data for monitoring purposes, and checking email and internet use and checking CCTV for criminal investigations, disciplinary and health and safety purposes in the case of an incident. This also appears in contracts of employment. Data will not be kept any longer than is necessary in line with NWHA’s Data Retention Policy.

NWHA will comply with the following requests for personal data:

* From agents authorised by the employee e.g. mortgage requests, references. The employee should confirm in writing that the information is to be released.
* For law enforcement (i.e. by the police for the prevention or detection of crime, assessment or collection of any tax or duty by HM Revenue and Customs, or the Child Support or Child Maintenance Agency). Disclosure is only allowed where failure to make the disclosure is likely to prejudice one of these purposes. In all cases the purpose of the request will be obtained in writing.
* For any other compulsory legal process.
* If urgently required, for the prevention of injury and damage to health.
* By trade union officials. The employee will be asked to confirm in writing.
* For any other compulsory legal process.
* If urgently required, for the prevention of injury and damage to health
* By specifically identified external sources, e.g. pension administrators, in order to administer internal benefit schemes.

Employees are entitled to see their personal data, but need to give HR reasonable notice to provide access. Employees are also entitled to know the purposes for which their personal data is intended to be used and the likely recipients (or class of recipients). The following information is excluded from disclosure:

* References received may be protected as disclosing information relating to identifiable third parties.
* Personal data used for management forecasting or planning if disclosure is likely to prejudice the conduct of that business or activity only.
* Records relating to any negotiations with the employee if disclosure is likely to prejudice those particular negotiations.
* If it involved disclosing information relating to an identifiable third party, unless the third party has consented or it is reasonable to comply without their consent. Failing these options, the data will be edited (‘redacted’) to protect the identity of third parties. Disclosure will be made if a health record is sought and the third party is a health professional who has compiled or contributed to it.

An employee will not be able to prevent processing necessary for the performance of a contract to which the employee is a party.

Personal information about an employee given to board members will be edited to remove all third party information.

**11. Suppliers and Contractors**

NWHA employs various contractors to carry out tasks and services on its behalf; some have a genuine need to use personal data of our residents. Such contractors are known as data processors.

If a contractor is likely to be a data processor, a standard set of clauses must be included in the tender document. These state basic requirements needed on the data protection status of the contractor. Full details are given in the Data Protection – Supplier Tender Clause and Agreement policy.

The contractor who is successful in winning the contract must enter into a Data Protection Processing Agreement that sets out the standards and obligations that NWHA expects in the processing of personal data. This longer agreement is also in the Data Protection – Supplier Tender Clause and Agreement policy.

Current contractors will also be required to sign an addendum to the contract to say that they will comply to GDPR and NWHA’s policies as they apply to the contract.

**12. Risk and Data Protection Impact Assessment**

There may be risks associated with the processing of particular types of personal data, which NWHA must assess by means of a Data Protection Impact Assessment (DPIA). A DPIA can cover in-house processing of personal data and that undertaken by other organisations on behalf of NWHA. See the Privacy Impact Assessment procedure.

New systems and technologies should be subject to examination that they have been designed to meet GDPR requirements; if not additional controls may be necessary. If the scope, nature, context and purposes of the processing are likely to result in a high risk to rights and freedoms, NWHA shall, prior to the processing, carry out a DPIA of the effect of the envisaged processing. A single DPIA may address a set of similar processing operations that present similar high risks.

Where, as a result of a DPIA it is clear that NWHA is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not NWHA may proceed must reviewed by the DPO. The DPO shall, if there are significant concerns, escalate the matter to the supervisory authority.

Appropriate controls may be selected from for example, ISO27001 (a set of Information security standards) and other good practice sources to reduce the risk to an acceptable level and reach GDPR compliance.

In order to protect employees and contractors from risk when working in residents’ homes, NWHA has a system to identify people who may threaten the safety of employees and others. This information is confidential and will not be disclosed outside NWHA unless it is required to ensure the health and safety of contractors and other suppliers. It will be subject to review and kept up to date and accurate.

**13. Security breaches**

Any employee who suspects a data protection breach, must report it immediately to the DPO, who will investigate following discussion with the Company Secretary, who will also deputise for the DPO in their absence. Serious breaches will be reported to the supervisory authority using the Breach Notification procedure.

A breach of security includes (but is not limited to):

* Divulging personal or sensitive personal data to an unauthorised person.

• Misuse of passwords or giving access to passwords.

• Misuse of personal or sensitive data or business sensitive information, even if accessed legitimately.

• Granting, gaining or attempting to gain unauthorised access to systems.

* Acting outside the Employee Code of Conduct and NHWA’s policies, procedures, advice and guidance from on data protection or information security.

• Accidental loss, damage or destruction of personal data.

**14. Records and Housekeeping**

**14.1 ‘Information Asset Register’**

NWHA has established an Information Asset Register to record processing activities of personal data, defining:

* purpose of the processing;
* the various steps involved in the processing;
* what data is being processed;
* who the data relates to;
* technical and organisational measures taken to secure the data;
* how consent is given/ processing gateway used.

Full details are given in the separate Information Asset Register procedure.

**14.2 Retention and disposal of data**

NWHA shall not keep personal data in a form that permits identification of data subjects for longer than NWHA deems necessary (in relation to the purpose(s) for which the data was originally collected).

NWHA may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Document and Data Retention policy, along with the criteria used to determine this period including any statutory obligations to retain the data.

Personal data must be disposed of in a way that protects the “rights and freedoms” of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the Document and Data Retention policy.

**15. Training**

All staff and board members will be required to read and understand this policy as part of their induction. Staff will be trained on a regular basis on this policy, including about their own rights. More detailed training on handling subject access requests in accordance with the Act will be given to relevant staff. The DPO will receive more specialised training.

**16. Monitoring and reporting**

The DPO monitors compliance with this policy and reports any breaches to the Company secretary. NWHA considers all personal information provided by its customers, staff or contractors as confidential, and any unauthorised disclosure is treated very seriously.

Deliberate breach of the policy is considered a serious disciplinary offence and may result in disciplinary action being taken which may in turn lead to dismissal. Staff may also face criminal liability in certain circumstances. Staff are required to notify the DPO where a breach of policy is suspected.

|  |  |
| --- | --- |
| **Linked policies**  **Policy** | **Date** |
|  |  |
| Data Retention Policy  *GDPR policies*  DP Privacy (and FPN) Policy  Supplier DP responsibilities Policy |  |

**Appendix A**

**Glossary of Definitions**

**Appendix A – Definitions**

**1 Breach of personal data** – 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. There is an obligation on the controller to report personal data breaches to the supervisory authority, where the breach is likely to adversely affect the personal data or privacy of the data subject.

**2 Child -** the GDPR defines a child as anyone under the age of 13 years old. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

**3 Consent by Data subject** - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

**4 Data Controller** – the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data.

**5 Data subject** – any living individual who is the subject of personal data held by an organisation.

**6 Establishment –** the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

**7 Filing system** – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. “Structured” covers any form of computer system or manual system which has a ‘fast indexing’ system.

**8 Material scope** **–** the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a ‘structured’ filing system or are intended to form part of a filing system.

**9 Personal data** – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It covers information about living people stored on a computer or in an organised paper filing system, CCTV system, digital camera or audio recordings and digital images.

**10 Processing -** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person’s performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

**11 Profiling** – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person’s performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

**12 Sensitive data/Special categories of personal data** – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**13** **Supervisory Authority** – the independent public authority established by a member state to administer and regulate the GDPR. The current UK authority is the Information Commissioners Office, which may continue with the same name and role for GDPR.

**14 Territorial scope -** the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

**15 Third party** – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.