Data protection and information governance policy

1.0 Purpose and scope

The purpose of this policy is to ensure that Notting Hill Genesis (NHG):

Complies with its legal obligations when handling personal information

- Assign clear responsibilities for data ownership within the organisation, driving data quality, automation & efficiency and innovation & improvement
- Ensure data quality for all data (personal and non-personal) is understood, measured and managed based on a clear business value prioritisation
- Support the creation and management of NHG's data catalogue
- Ensure NHG implements the most relevant data standards and conventions for its data to support interoperability and prevent lock-in

We regard the lawful and correct treatment of personal information and governed data assets as essential to the effectiveness and success of our operations and to maintaining trust between NHG and those with whom we carry out business. To this end we will process personal information lawfully and correctly by embedding this policy into our culture, processes and procedures.

This policy applies to all employees of NHG, partner agencies, third party contractors (including agency employees), volunteers and students or trainees on placement with NHG. NHG's Procurement Policy includes further information about how we ensure our business and supply chain are compliant with GDPR.

This policy applies to all personal data created or held by NHG, in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (e.g. ICT system/database, intranet, filing structure, email, filing cabinet, shelving and personal filing drawers).The General Data Protection Regulation (GDPR) has expanded the scope of applicable information to include 'the processing of personal data both automated and manual which form part of a filing system or are intended to form part of a filing system'. This is where the personal data are accessible according to specific criteria (for example this now includes chronologically ordered sets of manual records containing personal data).

The GDPR and the Data Protection Act 2018 (DPA) do not apply to information about deceased individuals, although NHG may owe a duty of confidentiality in relation to such information. The GDPR and the DPA do not apply to use of personal data purely for personal or household activities.

2.0 Definitions

Personal data – "any information relating to an identified or identifiable natural person ('the Data Subject'). An identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier"

The definition includes online identifiers such as an IP address and location data where they directly or indirectly identify individuals. Data which has been Pseudonymised (key coded) can also fall within the definition of personal data depending on how easy it is to attribute the pseudonym to a particular individual.

Data subject - The living individual who is the subject of the personal data.

Special category or sensitive personal data - previously referred to as sensitive data, this data requires extra protection, including personal data revealing:

- Any protected characteristic (for example CCTV images of individuals attending a place of worship or arrangements to allow a staff member to pray)
- Political opinions
- Religious or philosophical beliefs (for example veganism or atheism)
- Trade union membership
- Genetic or biometric data (for example fingerprints, DNA, voice recognition)
- Data concerning mental or physical health (for example sickness records, occupational health reports)
- Sex life
- Sexual orientation

Criminal convictions and offences data are not included as special category data although similar provisions for processing apply. All other criminal prosecutions data including investigations is dealt with separately under the Law Enforcement Provisions in the DPA and could be said to be 'extra special data'.

Controller - A person or entity who determines the purpose and the manner in which, personal data is to be processed. This may be an individual or an organisation and the processing may be carried out jointly with other persons.

Processor - A person who processes personal data on a controller's behalf. Anyone responsible for the disposal of confidential waste is also included in this definition.

Privacy Notice - A notice NHG is required to give before collecting personal data from data subjects. The Privacy Notice must contain certain information. See Appendix 1.

Profiling - Automated processing of personal data to evaluate certain aspects relating to data subjects in particular to analyse or predict behaviour, economic situation and personal preferences.

Information Commissioner's Office (ICO) - The UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Processing - obtaining, recording or holding the data or carrying out any operation or set of operations on data.

Information Asset Register - Part of NHG's records of processing. It details the data we hold, where it is held, who can access it, the risks to the data, security measures, who the data is shared with. Each Data owner is responsible for the section of Register relevant to their business area.

Data Catalogue – Provides a list of NHG's datasets, their quality level, key metadata fields, usage examples and access for users with the right permissions. The data catalogue integrates with the Information Asset Register (note this is separate to NHG existing Information Asset Register, and a product of growing levels of governed data assets)

Pseudonymisation - Personal data which can no longer be attributed to a specific data subject without the use of additional information. The data is kept separately from the personal data and is subject to security measures to ensure not attributed to data subject.

Confidential references – The falls within the scope of exemption under GDPR, it applies to references whether they are given or received as confidential reference for the purposes of prospective or actual:

- education, training or employment of an individual;
- placement of an individual as a volunteer;
- appointment of an individual to office; or
- provision by an individual of any service.

Criminal offence and convection - data that may be processed only under the control of official authority or where the processing is authorised by law that provides appropriate safeguards.

Data breach - 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 quality - – the fitness for purpose of data based on its accuracy, timeliness, completeness and consistency.

Data ethics – responsible and appropriate data use, based on the principles of transparency, accountability and fairness. NHG's approach is based on the government data ethics framework

3.0 The Data Protection Principles

We apply the six, legally enforceable, data protection principles. These principles are:

1. Lawfulness, fairness and transparency: personal data will be processed fairly, lawfully and in a transparent manner in relation to individuals. Personal data will not be processed unless at least one lawful basis has been met. For special category data this also requires at least one further condition to be met in addition to the lawful basis (see Appendix 1).

2. Purpose limitation: personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those processes.

3. Data minimisation: personal data is processed in a way that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

4. Accuracy: personal data is accurate and, where necessary, kept up to date. NHG takes every step to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

5. Storage limitation: personal data is kept in a form which permits identification of the data subjects for no longer than necessary for the purposes for which the personal data are processed. NHG has a Data retention policy and each department has a data retention schedule which specifies how long different categories of information will be kept for. Personal data will be stored in accordance with those retention periods.

6. Integrity and confidentiality: personal data will be 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.

The GDPR also introduces a further Accountability Principle which requires NHG, as Controller, to be responsible for, and be able to demonstrate, compliance with the above principles, including records of all processing of personal data. These records are kept in the Information Asset Register (IAR) and each Data owner is responsible for keeping the relevant section up-to-date and informing the Data Protection Team of any amendments or additions.

4.0 Data Governance Principles

We apply the four data governance principles. These principles are

1. Data is recognised as a priority: NHG recognises that data is a key asset which needs to be managed effectively to provide assurance and deliver insight for improved decision-making

2. Data is trusted: The ability to have trust in data is essential for deriving richer insights and for innovation and collaboration. Trust in data will only be achieved through a structured programme of data governance which improves data management principles including data quality. NHG's strategic aim is to ensure all of its corporate data and datasets held in any platform, is governed fully and comprehensively within the NHG Data Governance framework, whilst continuing to remain compliant with UK GDPR and any other Data Protection or Privacy regulations.

3. Data is owned: There is a clear framework in place to understand everyone's responsibilities with regards to NHG's data. Having clear data owners will unlock data to be accessed widely with an understanding of the wider impact data has beyond individual teams

4. Data is used in decision making: The goal of good data management and a strong governance process is to ensure data reaches everyone in the organisation and supports better decision making based on evidence.

5.0 Lawful basis for processing

We process personal data to carry out our functions but will only do this where there is a legal basis. We have adopted a minimalist risk appetite in relation to personal data processing. There are six lawful basis for processing and before processing personal data we will decide which is most appropriate. This depends on our purpose and the relationship that we have with the individual in question (the Data subject).

NHG's lawful basis for processing is covered in our Privacy Notice. It informs individuals on how NHG handles personal data. Staff will also follow the internal 'Consent guidance', which explains how to ensure that data protection principles are followed and adhered to.

1. Consent

Where NHG relies on the individual's consent alone this must be valid. Valid consent must be:

- Unambiguous (clearly given)
- Freely given (a genuine choice)
- Demonstrable (NHG is able to evidence the consent including when it was given)
- Specific (not bundled up in the small print)
- Informed (provided after being given all the information as to how the personal data will be processed, in the Privacy Notice, *see right to be informed below*)
- Explicit for special categories (in writing)
- No silence or inaction (NHG should not use opt-out boxes).

The individual must make a statement or a clear affirmative action to give valid consent, for example ticking a box, entering information or clicking on an icon.

If consent is being obtained from a child through online services and the child is under 13 years old, then parental consent is required.

NHG rarely rely upon consent as a legal basis for processing personal data and will consider other legal basis first.

2. Contract

In the large majority of cases we process personal data to:

- Fulfil our contractual obligations (e.g. as outlined in a tenancy of lease); or
- Do something before entering a contract (e.g. provide a quote).

The contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, NHG and the other party/parties intend them to be legally binding, and there is an element of exchange (usually an exchange of goods or services for money, but this can be anything of value).

The processing must be necessary to deliver NHG's side of the contract with a particular person (e.g. NHG keeps employees' details because the employee has a contract of employment). If the processing is only necessary to maintain NHG's business model more generally, this lawful basis will not apply and we would consider another lawful basis.

Legal obligation

We use this lawful basis when we need to process personal data to comply with a common law or statutory obligation. We identify the obligation in question, either by reference to the specific legal provision or by pointing to an appropriate source of advice or guidance that sets it out clearly (e.g. government website or industry guidance).

Vital interests

There is very limited scope to use this basis and it generally only applies to matters of life and death.

Public task

We consider the 'public task' basis first for most of our processing: "If you are a public authority and can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis." ICO guidance

This includes:

- Carrying out a specific task in the public interest which is laid down by law (statute or common law); or
- Exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law

Legitimate interest

This is the most flexible basis for processing and is most likely to be an appropriate basis where NHG use data in ways that people would reasonably expect and that have a minimal privacy impact.

Before using legitimate interest as lawful basis, NHG carry out a three-part test to assess whether a legitimate interest applies:

1. Purpose test: is NHG pursuing a legitimate interest?
2. Necessity test: is the processing necessary for that purpose?
3. Balancing test: do the individual's interests override the legitimate interest?

6.0 Roles and responsibilities

Under the GDPR and Data Protection Act NHG is a Data Controller.

Each department has:

- A Data owner
- A Data manager
- A Data steward
- Data consumers and creators

6.1 Roles

Data Protection Officer –They deliver the statutory functions required by GDPR, which involve:

- Inform and advise the Executive Board (EB) of their responsibilities under data protection legislation.
- Monitor NHG's compliance to data protection legislation and NHG's own policies in relation to data protection, information rights, information governance and security and records management
- Raise awareness and provide training to staff involved in processing personal data
- Provide advice on Data Protection Impact Assessment
- Have due regard to the risks associated with data processing activities
- Investigate any breaches of personal data and make recommendations for action and/or improvement
- Act as a point of contact for members of the public in relation to any issues regarding the processing of their personal data, in regards to the exercising of their rights.

The Data Protection Team (DPT) assists the DPO in delivering this statutory function and keeps a record of all incidents and breaches relating to the GDPR and the DPA. The team deals with all correspondence with the ICO relating to data protection matters.

Data owners - they have overall responsibility for overseeing and protecting data assets within their department. They have responsibility for:

- Leading a functional service area.
- Ensuring that personal data is safeguarded, with correct access limitations if stored internally, and ensuring appropriate due diligence is in place with suppliers if shared externally.
- Defining the expected data quality level and the cost to NHG, and improving data quality

- Championing data within department and across the business
- Monitoring risks
- Providing challenge and advice
- Maintaining their part of the IAR and declaring, on an annual basis that their business area is compliant with both GDPR and DPA
- Approving principles and methodologies to govern data and acting as the 'tie breaker' decision maker.

Data managers - they are responsible for:

- Maintaining a working knowledge and ensuring that personal data is safeguarded, with correct access limitations if stored internally, if shared externally accountable for ensuring appropriate due diligence is in place with suppliers.
- Ensuring standards/targets are achieved and that Subject Matter Expert understands their role and part to play
- Championing data within department, ensuring understanding the impact of its data assets data quality
- Manages DQ risks, initiates projects to address, advises Data Owner
- Ensuring that their department complies with GDPR, DPA and that it follows the Data governance and protection policy
- Monitoring data quality reports and driving the data quality agenda within the department
- Raising risks to the Data owner
- Setting up an agreed data management process based on the agreed corporate approach
- Deciding who can use data and how it can be used, assigning Data stewards and ensuring that data is properly managed within the department
- Deciding when there is a need to conduct a Data Protection Impact Assessment (DPIA) and understanding privacy rules
- Approving key data items that are managed, and having an overview of any processing activities that occur within their business area (including the repositories that hold personal data) and knowing the location of the primary source and location of slave data
- Ensuring that data assets have a description and purpose (providing more clarity for data owners and data stewards)

6.4 Data steward - they are responsible for:

- Identifying what data to gather, and bringing this together from a wide range of sources

- Learning about the business data, inside and outside of core systems, knowing where it is held, and uncovering how data can be used across departments.
- Maintaining a working knowledge of data protection, raising awareness to ensure that personal data is safeguarded and stored appropriately
- Establishing processes to update and maintain data
- Establishing standard data quality reporting utilising all available tools
- Acting as the point of contact for data-related issues
- Establishing processes to update and maintain data within their department, ensuring accuracy and consistency between systems and ensuring that staff are trained
- Promoting data integrity across departments and domains
- Communicating and enforcing both the Data governance and protection policy and the Subject Access Request Policy to their staff
- Ensuring standard data quality reporting
- Developing and enhancing data quality improvement plans
- Flagging issues and risks to their Data manager
- Producing metrics and key reports on data quality improvement progress.

Data consumers and creators - they are the people within NHG that use the organisation's data to deliver their day to day job or that input data on behalf of the organisation. They are responsible for:

- Defining what makes the data good enough to use
- Reporting data related issues that they unveil (without trying to address the issue themselves)
- Inputting data right first time.

6.2 Responsibilities

Head of Data Governance & Performance

They deliver the best practice function of data governance which involves:

- implement the data governance principles and ensure they are embedded in the business.
- Convene the Data Governance Steering Group with membership across the organisation. Support participants to understand their roles and responsibilities in data governance.
- Identify and put together plans for mitigating existing data governance risks and share with members of the Data Governance Steering Group

- Responsible for reporting to EB on data governance risks and issues including data quality scores

The data governance team assists the Head of Data Governance & Performance in delivering the data governance function through the implementation of data quality tools, understanding of business data and the technical challenges to adequately manage it.

Data Protection Team and Data Governance Team

NHG is responsible for ensuring that data within systems under the control of NHG cannot be accessed by unauthorised personnel. They also ensure that data cannot be tampered with, lost or damaged. IT isn't responsible for everything.

The Data Protection Team is responsible for providing day-to-day advice and guidance to NHG staff. They support NHG in complying with the GDPR, the DPA The Data governance and protection policy as well as the Subject Access Request policy.

The Data Governance Team is responsible for enabling the business to define, manage and improve the data it holds. They also support the business to publish governed, high-quality datasets for the rest of the organisation to access and use based on the right permissions and clearance.

7.0 Data sharing and third party's data processing

7.1 Engaging a supplier (Data Processor) to process personal data on behalf of NHG

If a contractor, partner organisation or agent of NHG is appointed or engaged to collect, hold, process or deal with personal data on behalf of NHG, we will ensure that adequate protections are in place to ensure that data is secure and the organisation complies with the requirements of the GDPR, by having a GDPR compliant binding contract is in place and a complete supplier checklist assessment.

If NHG is joint Controller with a partner organisation or agent, then we will, in a transparent manner, determine each controller's responsibilities under both the GDPR and the DPA and inform Data subjects of this where applicable. Unless the exchange of data does not involve personal data, a Data Sharing Agreement (DSA) is required and should be agreed and signed off by Data Protection Officer before any data is processed.

We promote information sharing and partnership working where it is in the best interests of the Data subject.

7.2 NHG's responsibilities as Data controllers to any Data processors (Suppliers/Contractors)

Our assessment of a competent data process considers the nature of the processing and what risks it poses to the data subject.

We will ensure that:

- Only processors that can guarantee that they will meet the requirements of the GDPR and protect the rights of data subjects

- A contract is in place that meets the requirements set out in GDPR

- We provide documented instructions for the processor to follow.

As Data controllers we remain directly liable for compliance with all aspects of the GDPR, and for demonstrating that compliance.

7.3 Engaging NHG as Data processor on behalf of a Data Controller

Where NHG is engaged by other organisations to process personal data, we become a Data processor and have obligations under GDPR relating to:

- Record-keeping
- Breach notification
- Contractual arrangements with sub-processors
- Data Protection Impact Assessments

7.4 Sharing personal data with a Data processor (Supplier)

When sharing personal data with data processors, we have a written data processing agreement in place. Such data processing agreement will provide, at a minimum, that the data processor shall:

- Comply with the instructions of the data controller
- Have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction, or accidental loss, alteration, unauthorised disclosure or access, and provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

This can either be a stand-alone data processor agreement or be in the form of data processing clauses that form part of a wider agreement between the parties.

We will also seek to include additional data provisions within the data processing agreement. (e.g. to ensure that data protection obligations are passed down the chain to any subcontractors of the data processor, obligations to assist the controller with any data breaches and with any requests by data subjects to access their personal data, an obligation on the data processor not to do anything that might put the data controller in breach of its obligation under the DPA).

Data processing agreements between data controllers and data processors will also stipulate that processors:

- Maintain written records of all processing activities carried out on behalf of NHG;
- Obtain NHG's consent to the appointment of a sub-processor (subcontractor); and
- Co-operate with NHG in the performance of its obligations under the GDPR (including notifying NHG of a personal data security breach without undue delay).

7.5 Sharing personal data within NHG

We process personal information for clearly established purposes which are clearly explained to the individual data subject.

Where data is intended to be shared within NHG, this will be made clear to the individual whose personal data is being collected (in the Privacy notice) and those with whom the data is shared will have a lawful reason in their own right for holding that data.

8.0 Rights of individuals and information access requests

Individuals have several rights in terms of the processing of their personal data. However, the lawful basis for processing determines which of these rights are available to data subjects (see the table below for examples):

Lawful Basis	Right to Erasure	Right to Portability	Right to Object
Consent	Yes	Yes	No
Contract	Yes	Yes	No
Legal Obligation	No	No	No
Vital Interests	Yes	No	No
Public Task	No	No	Yes
Legitimate Interests	Yes	No	Yes

NHG will comply with any exercise of individuals' rights within one month of receiving the request, or up to two months on grounds of complexity (the data subject must be told of the further time required within the initial one-month period).

Under the GDPR and the DPA, it is sometimes necessary to withhold certain information that has been requested by individuals in relation to the right to access.

8.1 Right to be informed

NHG's 'Privacy Notice' sets out the information that we must supply to the data subject and when they must be informed. The notice also provides more details on which lawful basis for processing NHG use.

This right does not apply when the data subject already has the information and in other limited circumstances set out by the GDPR where the personal data was supplied via a third party. See Appendix 2 for more detailed guidance.

8.2 Right to access

We provide personal data to the data subject free of charge unless the request is manifestly unfounded or excessive. We may also charge a fee to provide further copies of the same information. The fee is based on the administrative cost alone of providing the information. Further information is provided in our Subject Access Request Policy.

8.3 Right to rectification

Data subjects can ask us to rectify any inaccuracies in the personal data we hold about them (e.g. incomplete data). Where we have disclosed the personal information to a third party, we will also inform that third party of the rectification where possible. If we do not take any action in response to a request for rectification, we will notify the individual and inform them of their right to complain to the ICO.

We will respond to the request for rectification within one month. This can be extended a further two months where the request is complex.

8.4 Right to erasure (formerly the right to be forgotten)

This is not an absolute right and only applies in the following circumstances:

- Where the personal data is no longer required for its purpose (kept beyond its retention period)
- Where the data subject withdraws their consent and this is the only legal basis for processing
- Where the individual exercises their right to object to the processing and this is successful
- Where the personal data is being processed unlawfully (in breach of the GDPR and DPA)
- Where the personal data is erased to comply with a legal obligation
- Where the personal data relates to that of a child and is processed online with parental consent.

We can refuse to respond to a request for erasure where personal data is processed for the following reasons:

- To exercise the right to freedom of expression and information (only likely to be relevant to press releases made by NHG)
- To comply with a legal obligation or for the performance of a task carried out in the public interest or exercise of official authority, such as NHG exercising its powers and duties (although the information held will need to be still within its retention period)
- For public health purposes in the public interest
- Archiving purposes in the public interest, scientific research or statistical purposes or
- The exercise or defence of legal claims.

There are additional requirements when the request relates to children's personal data particularly online services, where they may not have been aware of the risks when they consented to the processing.

Where we have disclosed the personal data to third parties, we will inform them of the erasure, unless it is impossible or involves disproportionate effort.

8.5 Right to restrict processing

This right applies where data is held in limbo whilst challenges to its processing are resolved. The right is only relevant where:

- An individual disputes the accuracy of the personal data
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our organisation's legitimate grounds override those of the individual
- Where processing is unlawful but the individual objects to erasure or
- Where we have no further use for the data but an individual requires it for legal claims. In these circumstances NHG may store the personal data but not process it further (we will retain just enough information about the individual to ensure that the restriction is respected in the future).

8.6 Data portability

This right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way. It only applies to personal data which the individual has provided to us, where processing is based on consent or in performance of a contract and when processing is carried out by automated means.

We will provide the data free of charge within one month in a structured, commonly used and machine-readable form (e.g. open source file such as a CSV not PDF). If the request is complex, we may request an extension of two months. If the data subject requests it, we may transmit the data directly to another organisation, although only where this is technically feasible. If we are unable to comply, we let the individual know and inform them of their right to complain to the ICO.

8.7 Right to object

Individuals have a right to object to NHG processing personal information if that processing is:

- Based on legitimate interest or the performance of a task in the public interest or exercise of any official authority (for example NHG exercising its powers and duties)
- Direct marketing or any marketing including promoting the aims of an organisation directed to individuals
- For the purposes of scientific/historical research and statistics.

We will stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for processing which override the interest, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims.

Where applicable, we inform data subjects of their right to object at the first point of communication (e.g. in the privacy notice), when obtaining their personal data.

We stop processing data for direct marketing as soon as we receive an objection.

8.8 Rights related to automated decision making, including profiling

Automated individual decision-making is a decision made by automated means without any human involvement. Information is analysed to classify people into different groups or sectors, using algorithms and machine-learning. This analysis identifies links between different behaviours and characteristics to create profiles for individuals.

We inform our customers of the profiling and automated decision-making we carry out, what information we use to create the profiles and where we obtain this information from.

Automated decisions must not concern a child or be based on special categories of personal data unless:

- Explicit consent is obtained from the individual or
- Processing is necessary for reason of substantial public interest on the basis of a legal obligation with specific measures in place to safeguard the individual.

9.0 Disclosure of personal information about third parties

We do not disclose personal data about a third party except when in line with the GDPR and the DPA. Disclosure of personal data about a third party is done following the internal Third-Party Information Requests procedure.

Where we request the disclosure of personal data under the exemption criteria from a third party, officers will follow the internal Third party information requests procedure.

10.0 Privacy by Design

We implement safeguards to ensure the protection of personal data by default and from the outset of all projects. Safeguards such as technical and organisational security measures include pseudonymisation of data and data minimisation. Data protection by design is NHG's default position in relation to:

- Decision making
- Policy formulation
- Project management and
- Procurement.

11.0 Data Protection Impact Assessments (DPIA's)

NHG will carry out DPIAs in the following circumstances:

- High risk processing of personal data, particularly involving new technologies

- Profiling with significant effects on individuals
- Large scale special category/criminal data processing
- Public surveillance on a large scale (for example CCTV of a publicly accessible area).

Guidance on how to complete a DPIA can be found on Milo.

12.0 International transfers

We only transfer data to a third country (non-EU and non-EEA countries) when it has been judged by the ICO as 'Adequate Country' or where there are necessary safeguards in place with the organisation (e.g. a legally binding agreement between public bodies or contract clauses approved by the ICO). There is a list of 'Adequate Countries' available on the ICO's website.

13.0 Further information, enquires and complaints

Further information and guidance on data protection is available on the Information Commissioner's website at. www.ico.org.uk

Data subjects have the right to complain about the response they have received regarding their information right's request as well as to complain about other breaches of the GDPR or the DPA. All complaints should be written, dated and should include details of the complainant, as well as a detailed account of the nature of the problem.

Individuals under the right to be informed need to be provided (in the Privacy Notice) with the DPO's contact details being dataprotection@nhg.org.uk and their right to complain to the Information Commissioner's Office and their contact details being: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone: 01625 545 700 www.ico.org.uk

14.0 Breach of the Policy

Any breach of this policy will be investigated in line with NHG's internal Data breach procedure. We always treat any data breach as a serious issue.

Staff are expected to report any data breaches at the earliest opportunity. Notification will also be considered in any resulting disciplinary investigation, where the individual(s) concerned have assisted in the containment of the breach. Each incident will be investigated and judged on its individual circumstances in line with the Staff Code of Conduct.

Failure to comply may result in disciplinary action that may lead to dismissal, in addition to the possibility of an individual being criminally prosecuted under the GDPR and the DPA and/or liable to pay compensation in any civil action.

15.0 Data breach notification

Where a data breach affects individuals' rights and freedoms, we will report it to the Information Commissioner without delay and no later than within 72 hours.

If the risk to individual's rights and freedoms is high, we will also report the breach, without delay, to the individuals affected to which the personal data relates.

In reporting a data breach NHG staff will follow the NHG's internal Reporting data breaches procedure.

16.0 Policy Compliance

16.1 Compliance Measurement

We will regularly review organisational and technological processes to ensure compliance with both the GDPR and the DPA. We will also provide training to all staff processing personal data, which will be monitored and reported by the (Data Protection Team) DPT.

We will review compliance activity from the RSH, the Ombudsman and the Health & Safety Executive to ensure our approach to data governance reduces the risks and provides increased assurance

A list of the type of personal data held by each department is stored within a secure folder in SharePoint.

16.2 Non-Compliance

A deliberate or reckless breach of the GDPR or the DPA could result in a member of staff facing disciplinary action.

A deliberate or reckless breach of the data governance framework could result in a member of staff facing disciplinary action.

All personal data recorded in any format will be handled securely and appropriately, and staff will not disclose information for any purpose outside their normal work role. Any deliberate or reckless disclosure of information by a member of staff will be considered a disciplinary issue.

Deliberately or recklessly disclosing personal data without the authority of NHG is a criminal offence. It is also a criminal offence under DPA to re-identify personal data and processing this without the authority of NHG and to alter personal data to prevent disclosure. In addition civil actions may be brought against individuals and NHG for compensation.

Non-compliance of this Policy may also result in a report being made to the ICO which could result in council facing enforcement action, including substantial fines, in addition to substantial reputational damage.

Non-compliance with the data governance approach could expose NHG to regulatory risks such as a downgrade due to a lack of assurance of its data integrity.

16.3 Policy Review

This policy will be reviewed annually by the DPO and updated in the interim as required.

17.0 Related Policies, and Guidance

This Policy relates to other NHG policies and procedures, in particular:

- A Users Guide on when to use Email Encryption
- Consent Record Spreadsheet available on the GDPR webpage
- Data Breach Reporting Policy
- Data Privacy Impact Assessment (DPIA) guidance
- Information Sharing guidance available on the GDPR webpage
- Safeguarding Policy
- Staff Code of Conduct
- Member's Code of Conduct
- Retention Policy
- Information Security Policy
- ICT Data Classification, Handling and Retention Policy
- ICT Acceptable Use Policy
- Contract Management guidance available on the GDPR webpage
- Special category data and criminal offences data policy

Document control

Author	Bahzad Brifkani, Head of Data Protection
Approval date	3 February 2022
Effective date	9 September 2022
Approved by	Policy Group
Policy owner	Head of Data Protection, Head of Business Intelligence and Performance
Accountable Director	Director of Health and Safety and Business Services; Director of Business Improvement
Classification label	Policy is publicly available and on request

Version Control

Date	Amendment	Version
3/2/2022	New policy	1.0

9/9/2022	Added links to internal procedures; changed the review cycle from every two years to annually; added a classification label; added statement on risk appetite	1.1
6/4/23	Added statement to point 2 in section 4 around NHG's strategic aim	1.2

Appendix 1 - Additional Conditions for processing special category data

Processing is necessary for:

- Legal obligations in employment law, social security and social protection law to protect vital interests
- Carried out by a not-for-profit body with a political, philosophical, religious or train union aim
- Relates to personal data made manifestly public by the data subject
- For the establishment, exercise or defence of legal claims
- Public interest as permitted by law
- Preventative or occupational medicine
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or
- The data subject has given their explicit consent.

Appendix 2-GDPR and Data Protection Policy

What information must be supplied in a Privacy Notice?	**Data obtained directly from data subject**	**Data not obtained directly from data subject (for example via a third party organisation**
Identity and contact details of the controller (NHG) or the joint controllers (NHG and others) and the data protection officer's contact details: dataprotection@nhg.org.uk	✓	✓
Purpose of the processing and the lawful basis for the processing (see Definitions section)	✓	✓

The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data	✓	✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards, if applicable.	✓	✓
Retention period or criteria used to determine the retention period (see retention schedules)	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant (only where legal basis is Consent)	✓	✓
The right to lodge a complaint with the ICO	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources	✓	✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of any automated decision making, including profiling and information about how decisions are made, the significance and the Consequences	✓	✓
When should information be provided?	At the time the data are	At the time the data are
		If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
		If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

Appendix 3 Examples of exemptions to the non-disclosure of third party personal data -

1. Crime and Taxation
1. National security
2. Defence
3. Prevention, detection and prosecution of criminal offences
4. Enforcement of civil matters
5. Disclosures required by law
6. Statement made by health, education and social care professionals

Examples of exemptions to the right of access:

- Legal professional privilege
- Corporate finance- effecting markets and prices
- Management forecasts
- Negotiations