General Data Protection Regulation Policy

Outline

This policy gives important information about:

- the data protection principles with which NRW must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, eg about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

Statement and Purpose

NRW obtains, keeps and uses personal information (also referred to as data) about members of the public, other third parties, current and former employees, temporary and agency workers, contractors, and volunteers for a number specific lawful purposes.

This policy sets out how we comply with our data protection obligations and seek to protect personal information. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce, and how (and when) we delete that information once it is no longer required.

The Data Protection Officer is responsible for informing and advising NRW on its data protection obligations, and for monitoring compliance with those obligations. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Data Protection Officer [set out details of how DPO can be contacted, eg email and telephone number].

Scope

This policy applies to all NRW staff, contractors and agency staff undertaking work on behalf of NRW including temporary and agency workers and volunteers and to all Personal Data processed by us at any time, by any means and in any format, and all methods of holding and storing the information including but not limited to:

- Manually stored paper data

- Email accounts
- Data held in computer applications and databases
- Data from CCTV and other audio or visual recording systems including tapes
- Data held in records archive storage
- Data held on CD, memory stick etc.

Staff should refer to other relevant policies including in relation to [internet, email and communications, monitoring, social media, information security, data retention, and criminal record information, Data Protection Impact assessment and Privacy noice, which contain further information regarding the protection of personal information in those contexts.

Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

Data protection principles

NRW will comply with the following data protection principles when processing personal information:

- we will process personal information lawfully, fairly and in a transparent manner;
- we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;
- we will keep personal information[in a form which permits identification of data subjects] for no longer than is necessary for the purposes for which the information is processed; and
- we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Basis for Processing Personal Information

In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, ie:
    - that the data subject has consented to the processing;
    - that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - that the processing is necessary for compliance with a legal obligation to which NRW is subject;
    - that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
    - that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
    - that the processing is necessary for the purposes of legitimate interests of NRW or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject
- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (ie that there is no other reasonable way to achieve that purpose);
- document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
- where sensitive personal information is processed, also identify a lawful special condition for processing that information, and document it; and
- where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

Sensitive personal information

Sensitive personal information is sometimes referred to as ‘special categories of personal data’ or ‘sensitive personal data’.

NRW may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

- we have a lawful basis for doing so, eg it is necessary for the performance of the employment contract, to comply with NRWs legal obligations or for the purposes of NRWs legitimate interests; and
- one of the special conditions for processing sensitive personal information applies, eg:
    - the data subject has given has given explicit consent;
    - the processing is necessary for the purposes of exercising the employment law rights or obligations of NRW or the data subject;
    - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
    - processing relates to personal data which are manifestly made public by the data subject;
    - the processing is necessary for the establishment, exercise or defence of legal claims; or
    - the processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, staff must notify the data protection officer of the proposed processing, in order that the data protection officer may assess whether the processing complies with the criteria noted above.

Sensitive personal information will not be processed until:

- the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

In relation to sensitive personal information, NRW will comply with the procedures set out in the above paragraphs to make sure that it complies with the data protection principles.

Data protection impact assessments (DPIAs)

Where processing is likely to result in a high risk to an individual's data protection rights (eg where NRW is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

Before any new form of technology is introduced, the manager responsible should therefore contact the data protection officer in order that a DPIA can be carried out.

Documentation and records

We will keep written records of processing activities which are high risk, ie which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

- the name and details of the relevant organisation (and where applicable, of other controllers, and the DPO);
- the purposes of the processing;
- a description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;

- where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- where possible, retention schedules; and
- where possible, a description of technical and organisational security measures.

As part of our record of processing activities we document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal information;
- DPIAs; and
- records of data breaches.

If we process sensitive personal information or criminal records information, we will keep written records of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- the lawful basis for our processing; and
- whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

- carrying out information audits to find out what personal information NRW holds; and
- reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

Roles and Responsibilities

All staff are responsible for helping NRW to meet its data protection obligations.

If you have access to personal information, you must:

- only access the personal information that you have authority to access, and only for authorised purposes;
- only allow other staff to access personal information if they have appropriate authorisation;
- only allow individuals who are not NRW staff to access personal information if you have specific authority to do so from the data protection officer
- keep personal information secure (eg by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in NRWs information security policy);
- not remove personal information, or devices containing personal information (or which can be used to access it), from NRWs premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- not store personal information on local drives or on personal devices that are used for work purposes

You should contact the data protection officer you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information
- any data breach
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from NRWs premises without appropriate security measures being in place;
- any other breach of this policy or of any of the data protection principles

Information Security

NRW will use appropriate technical and organisational measures in accordance with NRWs policies to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

- making sure that, where possible, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where NRW uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of the NRW;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the NRW and under a written contract;
- the organisation will assist NRW in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist NRW in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to NRW as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide NRW with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell NRW immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the data protection officer

Storage and retention of personal information

Personal information (and sensitive personal information) will be kept securely in accordance with NRWs [information security policy].

Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow NRWs [records retention policy] which sets out the relevant retention period. Where there is any uncertainty, staff should consult the data protection officer.

Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely

Data Breaches

A data breach may take many different forms, for example:
loss or theft of data or equipment on which personal information is stored;

- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

NRW will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

International Transfers

We will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

Training

NRW will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests

under this policy, will receive additional training to help them understand their duties and how to comply with them.

Consequences of failing to comply

NRW takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal information is being processed; and
- carries the risk of significant civil and criminal sanctions for the individual and NRW; and
- may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with any requirement of it will be treated as a breach of the NRW Code of Conduct.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the data protection officer

The Security Officer is responsible for managing and investigating any actual or suspected unauthorised disclosures of Personal Data and recommending measures to prevent the reoccurrence of such incidents and breaches.

ICT is responsible for advising the business on the technical measures and controls required to protect the security of Personal Data processed by NRW and to provide a secure network and ICT equipment.

Internal Audit is responsible for auditing the business processes, operating procedures and working practices of NRW and its service providers which affect the processing of Personal Data, to monitor compliance with this policy.

Other relevant information

Organisations that have a crime prevention, law enforcement or tax collection function such as the Police, Revenue and Customs or Department of Work and Pensions may require Personal Data held by NRW for the prevention or the detection of a crime, NRW may be able to release this information by applying an exemption under GDPR. Should you receive any such request, the Data Protection Officer must be notified in advance
NRW Policies, Procedures and Guidance:

CCTV
Clear Desk
DMS
Email
ICT security
Privacy notice
Data Protection Impact Assessments (DPIA)
Remote Access
Removable Media
Retention schedule
Secure disposable
Security Classifications
Security Policy

Security Data and Information Incidents
Subject Access Request

Contact
Senior Data Protection Officer

Approval
Director of Governance

Version
Version 1. Published May 2018

For first review in 6 months and then every two years. Amendments will be made sooner where a relevant change in legislation or business requirement occurs and following discussion with the representing Trade Unions.