General Data Protection Regulation Policy

Statement and Purpose

One of our values as an organisation is that we care for each other and the people that we work with. This is why we want to maintain a safe and secure work environment for all of us as staff and those affected by our work.

The purpose of this policy is to outline how NRW and its employees maintain legal compliance in the security of personal data in line with UK legislation.

Compliance

This policy is required to maintain compliance with the Data Protection Act (2018) and the General Data Protection Regulation (GDPR).

The organisation can be audited and inspected following a data breach by the Information Commissioners office who have the ability to issue penalties of up to €20 Million, in proportion to the seriousness of the data breach.

Scope

This policy applies to all NRW staff, contractors, agency/temporary workers and volunteers undertaking work on behalf of NRW. It relates to all personal data processed, held and stored by NRW at any time in any format, 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.

Key principles

The GDPR sets out 7 key principles which lie at the heart of the data protection regime. These are:

- Lawfulness, fairness and transparency of processing;
- Purpose limitation;
- Data minimisation;
- Accuracy;

- Storage limitation;
- Integrity and confidentiality (security);
- Accountability.

Roles and Responsibilities

The Data Protection Officer (DPO) – This role is embedded within the role of the Lead Specialist Advisor, Information Management and Security. The DPO is responsible for implementing and upholding this policy. They inform and advise NRW on its data protection obligations and monitor the organisations compliance against these obligations.

The Senior Information Risk Owner (SIRO) - The single individual who is accountable for the organisations approach to information risk including security, quality and availability. This is a Director role within the organisation and is the point of contact for Information Asset Owners reporting and assurance.

Information Asset Owners (IAO) - Accountable for the data and information which falls under their area of work. Their role is to ensure the security, quality, availability and use of the data and information assets they are accountable for. They are the highest-level decision maker for information relating to their work area and are required to ensure sufficient resources are available to manage data and information appropriately. Every dataset must fall under one information asset with an accountable IAO. IAOs will provide assurance to the SIRO.

Data Custodian (DC) – The accountable individual for a data asset (dataset). This will be someone for whom data management is a key part of their role. They will be the lead user or main point of contact for the dataset, usually a single member of staff, although potentially more where an equal level of responsibility for a dataset rest with more than one person. The Data Custodian will be the main point of contact for the IAO and will provide assurance to the IAO that the data are being managed appropriately. They must report any issues or potential breaches promptly. Every dataset must have one or more Data Custodian.

Data user/editor - Any member of staff who works with data as part of their role. They will normally be someone who uses data as a part of their work, as opposed to working with data being the key focus of their role. This can be someone who works with data at any point of the data lifecycle e.g. entering, updating, viewing, reporting etc.

All NRW Staff and Contractors – Everyone has a responsibility to comply with the policies and procedures outline for the protection of personal data, for informing the DPO of any suspected data breach as soon as possible and following the correct measures if new data is to be obtained, stored or processed in anyway.

Other relevant information

What else should we know in relation to this policy – any supporting detail necessary?

Are there procedures (insert the link) that need to be followed?

Other sources of information

For further guidance on the Data Protection Act (2018) and GDPR please refer to the ICO website https://ico.org.uk/

Equality and Diversity

We are committed to a culture of equality, diversity and inclusion. We aim to ensure that no-one receives less favourable treatment on the grounds of their age, disability, gender reassignment, being married or in a civil partnership, pregnancy, race, sex, sexual orientation or religion, belief or non-belief.

An Equality Impact Assessment has not been produced for this Policy

Contact

This policy and related procedure are owned by – Lead Specialist Advisor, Information Management and Security.

Approval

Approved by: Senior Information Risk Owner (SIRO)

Version

Version 2 - Published February 2021

First published - May 2018

Review Period - every two years. Amendments will be made sooner where a relevant change in legislation or business requirement occurs and following discussions with the representing Trade Unions.