



Data Protection Policy

Alastair Taylor - CEO

NYnet Limited, 80 High Street, Harrogate, HG2 7LW.
Registered in England & Wales No. 06069791. VAT No. GB 123 4070 56.
NYnet is a UK limited company controlled by North Yorkshire County Council.

Telephone: +44 (0)1423 598210

Website: www.nynet.co.uk

Email: enquiries@nynet.co.uk



Contents

Introduction and Scope	4
Roles and Responsibilities	4
Data Protection Principles	5
Lawful Bases.....	5
Data Subject Rights	5
Records of Processing	6
Privacy by Design and Risk Assessments	6
Information Sharing.....	7
Contract Management.....	7
Records Management.....	7
Training.....	8
Complaints	8
Appendix One – Appropriate Policy Document (APD)	10
Appendix Two – Subject Access Requests (SARs)	13
Appendix Three – Freedom of Information (FOI) and Environmental Information Regulation (EIR) Requests.....	14
Appendix Four-Surveillance Policy.....	15

Introduction and Scope

This policy is to ensure that NYnet complies with the requirements of the UK General Data Protection Regulation, the Data Protection Act 2018, Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation.

This policy including its appendices applies to its entire workforce. This includes employees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, NYnet. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

This policy is the organisation's main information governance policy and applies to all personal data, regardless of whether it is in paper or electronic format. It should be read alongside the Information Security policy.

Roles and Responsibilities

Personal data will be processed in accordance with the requirements of UK GDPR and in compliance with the data protection principles specified in the legislation. Overall responsibility for ensuring that the organisation meets the statutory requirements of any data protection legislation lies with the Board of Directors. The following roles have day to day responsibility for compliance and provide the necessary assurance to the Board.

Data Protection Officer (DPO)

The role of the DPO is to assist the organisation in monitoring compliance with the UK GDPR and the Data Protection Act 2018 and advise on data protection issues. NYnet have appointed Veritau as its DPO. Veritau's contact details are:

Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA



information.governance@veritau.co.uk // 01904 552848

The DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;
- Facilitating a periodic review of the corporate Information Asset Register and information governance policies;
- Assisting with the reporting and investigation of information security incidents;
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- Reporting to the Senior Management Team on the above matters.

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who has ultimate responsibility for operational risk, ensuring that the organisation's policies and procedures are effective and comply with legislation, and promoting good practice. At NYnet this role lies with the Chief Executive

Single Point of Contact (SPOC)

The SPOC is someone at operational level who can take responsibility for data protection, including communicating with data subjects and the DPO. At NYnet this role lies with the Office Manager.

Information Asset Owner (IAO)

An IAO is an individual who is responsible for the security and maintenance of a particular information asset. They are responsible for ensuring that other members of staff are using the information safely and responsibly. NYnet will ensure that IAOs are appointed based on sufficient seniority and level of responsibility, and document this in its Information Asset Register (IAR).

All staff

All staff, including contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the organisation are responsible for collecting, storing and processing any personal data in accordance with this policy.

Data Protection Principles

NYnet will comply with the data protection principles, as defined in Article 5 of the UK GDPR. NYnet will ensure that personal information is:

- Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).
- Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**Data Minimisation**).
- Accurate and where necessary kept up to date (**Accuracy**).
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (**Storage Limitation**).
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

NYnet recognises that not only must it comply with the above principles, it must also demonstrate its compliance (**Accountability**).

Lawful Bases

UK GDPR sets out several conditions under which NYnet can process personal information lawfully. NYnet usually rely on the lawful basis of Contract or Legal Obligation, however at times it may rely on its legitimate interests. NYnet will only do this where it is using data in ways individuals would reasonably expect and will carry out an appropriate legitimate interest assessment (LIA) prior to starting the processing.

NYnet have an Appropriate Policy Document (APD) in place (see Appendix One) which provides information about its processing of special category (SC) and criminal offence (CO) data. The APD demonstrates how NYnet comply with the requirements of the UK GDPR and DPA.

Data Subject Rights

Under the UK GDPR, individuals have several rights in relation to the processing of their personal data:

Right to be informed

NYnet provide individuals with privacy information at the time it collects their data, normally by means of a privacy notice, which is made easily accessible to the data subject. Privacy notices will be clear and transparent, regularly reviewed, and include all information required by data protection legislation.

Right of access

Individuals have the right to access and receive a copy of the information NYnet holds about them. This is commonly known as a Subject Access Request (SAR). NYnet has in place a SAR procedure which details how it deals with these requests (Appendix Two).

Other rights include the right to rectification, right to erasure, right to restrict processing, right to object, right to data portability and rights related to automated decision-making, including profiling.

Requests exercising these rights can be made to any member of staff, but NYnet encourages requests to be made in writing, wherever possible, and forwarded to the SPOC – sally.weatherill@nynet.co.uk who will acknowledge the request and respond within one calendar month. Advice regarding such requests will be sought from NYnet's DPO where necessary.

A record of decisions made in respect of the request will be retained; recording details of the request, whether any information has been changed, and the reasoning for the decision made.

Records of Processing

In accordance with Article 30 of UK GDPR, NYnet must keep a record of its processing activities. NYnet will do this by developing and maintaining an Information Asset Register (IAR) which will include as a minimum:

- The organisation's name and contact details,
- The name of the information asset,
- The owner of that asset, known as the Information Asset Owner (IAO),
- The purposes of the processing,
- A description of the categories of individuals and the types of personal data,
- Who has access to the personal data, and who it is shared with,
- The lawful bases for each processing activity,
- The format and location of the personal data,
- Details of any transfers to third countries, and the appropriate safeguards,
- The retention periods for each asset,
- A general description of the technical and organisational security measures.

NYnet will include links to relevant documentation, such as data processing contracts, information sharing agreements, and risk assessments, wherever possible.

NYnet will review the IAR at least annually to ensure it remains accurate and up to date, consulting with the DPO as necessary.

Privacy by Design and Risk Assessments

NYnet will adopt a privacy by design approach and implement appropriate technical and organisational security measures to demonstrate how it integrates data protection into its processing activities.

NYnet will conduct a Data Protection Impact Assessment (DPIA) when undertaking new, high-risk processing, or making significant changes to existing data processing. The purpose of the DPIA is to

consider and document the risks associated with a project prior to its implementation, ensuring data protection is embedded by design and default.

All of the data protection principles will be assessed to identify specific risks. These risks will be evaluated and solutions to mitigate or eliminate these risks will be considered. Where a less privacy-intrusive alternative is available, or the project can go ahead without the use of special category data, NYnet will opt to do this.

All DPIAs are signed by NYnet's Senior Information Risk Owner and Data Protection Officer.

Information Sharing

In order for NYnet to effectively fulfil its duties it is sometimes necessary for it to share information with third parties. Routine and regular information sharing arrangements will be documented in NYnet's privacy notices and in its IAR.

Any further or ad-hoc sharing of information will only be done so in compliance with legislative requirements, including the ICO's data sharing code of practice. NYnet will only share personal information where it has a lawful basis to do so, ensuring any disclosure is necessary and proportionate. All disclosures will be approved by the relevant staff member and recorded in a disclosure log.

Contract Management

All third-party contractors who process data on NYnet's behalf must be able to provide assurances that they have adequate data protection controls in place. Where personal data is being processed, NYnet will ensure that there is a written contract in place which includes all the mandatory data processing clauses, as required by UK GDPR.

NYnet will maintain a record of its data processors, and regularly review the data processing contracts, with support from the DPO, to ensure continued compliance.

International Transfers

Usually, personal information processed by NYnet is not transferred outside of the European Economic Area (EEA), which is deemed to have adequate data protection standards by the UK government. If personal data is transferred outside the EEA, NYnet will take reasonable steps to ensure appropriate safeguards are in place.

NYnet will consult with the DPO for any processing which may take place outside of the EEA prior to any contracts being agreed.

Records Management

A programme is in place for managing NYnet's records throughout their lifecycle, including using methods such as version control and file plans to ensure that records can be easily searched and accessed in the event of an information request.

Email management

NYnet have a process in place to ensure that emails are also managed in line with this policy and its retention schedule. Emails discussing organisational business or reflecting significant actions or decisions concerning organisational business will not be stored in personal email inboxes but will be removed and stored securely in the appropriate filing system.

Personal email inboxes are regularly reviewed by staff to ensure any unnecessary emails are deleted.

Storage and security

All records, especially where containing personal data, will be stored securely to maintain confidentiality, whilst also keeping information accessible to those authorised to see it. Electronic records will have appropriate security and access controls in place, and systems will have robust audit functions in place wherever possible.

Paper records will be stored in secure, lockable storage areas with restricted access.

When sharing or transferring records containing personal information, NYnet will ensure appropriate transmission security controls are in place, in line with its Classification and Handling Policy.

Retention and disposal

The retention period for particular types of records is determined by legal, regulatory or functional requirements. NYnet have adopted the Documents and Records Retention Policy, this can be found on Activ.

NYnet will ensure that any records containing personal or confidential information are disposed of appropriately and securely when they have reached the end of their retention period.

Records held in databases or electronic management systems with the functionality for automatic destruction of records after a specified period of time will be used wherever possible. A review of the records will be carried out prior to destruction, where practical.

Where automatic disposal is not in place, for example for paper records, NYnet will carry out a manual review, at least annually, to ensure they are deleted in line with retention guidelines.

The disposal of all information is documented to ensure that NYnet maintain a record of when it has been deleted and by whom. This allows NYnet to evidence that a record no longer exists in the event of a subject access or Freedom of Information request being received.

Training

NYnet will ensure that appropriate guidance and training is given to its workforce and other authorised users on data protection, records management and access to information. Training will be delivered as part of the induction process and as refresher training at appropriate intervals.

Specialised roles or functions with key data protection responsibilities, such as the SIRO, SPOC and IAOs, will also receive additional training specific to their role.

NYnet will keep a record of all training that has been completed and ensure that data protection awareness is raised in staff briefings and as standard agenda items in meetings, where appropriate.

NYnet will ensure that any third-party contractors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

Complaints

NYnet take complaints seriously, and any concerns about the way it has handled personal data or requests for further information in relation to data protection, should be raised with the SPOC (sally.weatherill@nynet.co.uk). NYnet will then liaise with the DPO, where necessary, for advice and guidance.

If an individual remains dissatisfied after NYnet have concluded its investigation, they may complain to the Information Commissioner's Office. Their contact details are below:

Phone: 0303 123 1113 or via their [live chat](#). Their normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on [Contact us | ICO](#).

Appendix One – Appropriate Policy Document (APD)

Introduction

NYnet processes special category and criminal conviction data in the course of fulfilling its functions. Schedule 1 of the Data Protection Act 2018 requires data controllers to have in place an 'appropriate policy document' where certain processing conditions apply for the processing of special categories of personal data and criminal convictions data. This policy fulfils this requirement.

This policy complements NYnet's existing records of processing as required by Article 30 of UK General Data Protection Regulation, which has been fulfilled by the creation and maintenance of an Information Asset Register. It also reinforces NYnet's existing retention and security policies, procedures and other documentation in relation to special category data.

Special categories and conditions of processing

NYnet process the following special categories (SC) of data:

- health.

NYnet also process criminal offence (CO) data under Article 10 of UK GDPR, including for pre-employment checks and declarations by employees in line with their contractual obligations.

NYnet rely on the following processing conditions under Article 9 of UK GDPR and Schedule 1 of the Data Protection Act 2018 to lawfully process special category and criminal convictions data:

Article 9(2)(b) – employment, social security or social protection

To comply with NYnet's legal requirements as an employer and safeguard its staff, NYnet need to collect some special category data.

Examples include when it carries out DBS checks to evidence suitability for a role and collect medical information to put in reasonable adjustments at work and monitor staff absence.

When processing information under Article 9(2)(b), NYnet also require a Schedule 1 condition under the Data Protection Act 2018. The condition it relies on for this processing is **Schedule 1, Part 1, (1) - employment, social security and social protection**.

Article 9(2)(h) – health or social care purposes

NYnet relies on this lawful basis when processing information in relation to occupational health and, assessing the working capacity of an employee.

When processing data under Article 9(2)(h), it also requires a Schedule 1 condition under the Data Protection Act 2018. The conditions NYnet rely on for this processing are **Schedule 1, Part 1, (2) – health and social care purposes**.

Compliance with Data Protection Principles

NYnet have several policies and procedures in place to ensure its compliance with the Article 5 Data Protection Principles and meet its accountability obligations, explained in more detail below:

Accountability principle

NYnet have put in place appropriate technical and organisational security measures to meet the requirements of accountability. These include:

- The appointment of a Data Protection Officer, Veritau, which provides reports to the Board.
- Taking a data protection by design and default approach to NYnet's processing activities, including the use of risk assessments.
- Maintaining documentation of NYnet's processing activities through an Information Asset Register.
- Adopting and implementing information governance policies and ensuring NYnet have written contracts in place with data processors.
- Implementing appropriate security measures in relation to the personal data NYnet process. More detail can be found in the Information Security Policy.

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. NYnet have identified an appropriate Article 6 condition and also, where processing SC or CO data, an Article 9 and Schedule 1 condition.

NYnet consider how any processing may affect individuals concerned and provide clear and transparent information about why it processes personal data, including the lawful bases, in its privacy notices and this policy document. All privacy notices provide details of data subject rights. NYnet privacy information is regularly reviewed and updated to ensure it accurately reflects its processing.

Principle (b): purpose limitation

Personal data is only processed to allow NYnet to carry out the necessary functions and services it is required to provide in line with legislation. NYnet clearly set out its purposes for processing in its privacy notices, policies and procedures, and in its IAR. If NYnet plan to use personal data for a new purpose, other than a legal obligation or function set out in law, NYnet check that it is compatible with its original purpose, or it obtains specific consent for the new purpose.

Principle (c): data minimisation

NYnet only collect the minimum personal data needed for the relevant purposes, ensuring it is necessary and proportionate. Any personal information that is no longer required, especially where it contains special category data, is anonymised or erased.

Principle (d): accuracy

Where NYnet become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is processed, NYnet will take every reasonable step to ensure that data is erased or rectified without delay. Where NYnet are unable to erase or rectify the data, for example because the lawful basis it relies on to process the data means these rights do not apply, NYnet will document its decision. Where NYnet have shared information with a third party, it will take all reasonable steps to inform them of the inaccuracies and rectification. NYnet maintain a log of all data rights requests and have appropriate processes for handling such requests.

Principle (e): storage limitation

NYnet have implemented a Retention Schedule. Where there is no legislative or best practice guidance in place, the SIRO will decide how long the information should be retained based on the necessity to keep the information for a legitimate purpose or purposes. NYnet also maintain a Destruction Log, which documents what information has been destroyed, the date it was destroyed and why it has been destroyed.

Principle (f): integrity and confidentiality (security)

NYnet employ various technical and organisational security measures to protect the personal and special category data that it processes. Further details of security measures can be found in the Information Security policy and associated documents in the ISMS.

In the event of a personal data breach the incident will be recorded on a log, investigated, and reported to NYnet's Data Protection Officer where necessary. High risk incidents are reported to the Information Commissioner's Office. This process is documented in greater detail in the Information Security policy.

Retention of special category and criminal convictions data

The retention periods of special category and criminal convictions data are set out in the Retention Schedule. Retention periods of specific information assets are identified in the Information Asset Register.

Appendix Two – Subject Access Requests (SARs)

Under the UK GDPR, individuals have the right to make a Subject Access Request (SAR) to any member of NYnet's workforce, contractor or agent working on behalf of NYnet. Requests need not be made in writing, but NYnet encourage applicants to do so where possible. Requests should be forwarded to the SPOC who will log the request and acknowledge it within five working days.

NYnet must be satisfied of the requestor's identity and may have to ask for additional information to verify this, such as:

- valid photo ID, such as driver's licence or passport,
- proof of address, such as a utility bill or council tax letter,
- confirmation of email address, or
- further information for NYnet to be satisfied of the applicant's identity.

Only once NYnet is confident of the requestor's identity and have sufficient information to understand the request will it be considered valid. NYnet will then respond to the request within the statutory timescale of one calendar month.

NYnet can apply a discretionary extension of up to a further two calendar months to comply if the requested information would take a considerable amount of time to respond, due to either the complexity or volume of the records. If NYnet wish to apply an extension, it will firstly seek guidance from its DPO, then inform the applicant of the extension within the first calendar month of receiving the request.

If NYnet think it necessary to apply any exemptions, it will seek guidance from its DPO. In limited circumstances, NYnet may also refuse a request on the basis that it is manifestly unreasonable or excessive.

Internal Review

Complaints in relation to SARs and other data subject rights will be processed as an internal review request.

An internal review will be dealt with by an appropriate member of staff who was not involved in the original request. They will examine the original request and response and decide whether it was dealt with appropriately under the legislation. The reviewing officer will decide whether to uphold or overturn any exemptions. A full response will be provided within one calendar month where possible.

If an individual remains dissatisfied after NYnet has concluded its investigation, they may appeal to the Information Commissioner's Office. Their contact details are below:

Phone: 0303 123 1113 or via their [live chat](#). Their normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on [Contact us | ICO](#).

Appendix Three – Freedom of Information (FOI) and Environmental Information Regulation (EIR) Requests

Freedom of Information (FOI)

The Freedom of Information Act 2000 (FOIA) is part of the Government's commitment to greater openness and transparency in the public sector. It enables members of the public to scrutinise the decisions of public authorities more closely and ensure that services are delivered properly and efficiently. NYnet have two main responsibilities under the Freedom of Information Act:

- To publish certain information about its activities in a publication scheme, and
- To process and respond to individual requests for information, with a duty to provide advice and assistance.

Under FOI, anyone can request access to general recorded information NYnet holds. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. A Code of Practice under section 45 of the Act sets out recommendations for the handling of requests for information. To comply with this Code requests must:

- Be in writing,
- Provide the name or company name and contact address or email address,
- Describe the information they are requesting,
- Ideally, state the preferred format they would like the information to be provided.

Any request that cannot be answered promptly as part of normal day to day business or where NYnet are asked to handle it under Freedom of Information, will be treated as a FOI request.

Information can be withheld if one or more of the 24 exemptions within the FOIA apply. This could mean that certain information is not released in response to a request or is not published. Requests for information can be refused for reasons including:

- The information is not held
- It would cost too much or take too much staff time to comply with the request
- The request is considered vexatious
- The request repeats a previous request from the same person.

Environmental Information Regulations (EIR)

Requests for information that relates to the environment, including activities which may affect the environment, are dealt with under the Environmental Information Regulations 2004. EIR is similar to FOI but there is an even greater presumption of disclosure, and there are fewer exceptions under which a request can be refused. Requests under EIR can also be given verbally and do not need to be in writing, but must include:

- A name or company name and contact address or email address,
- A description of the information being requested,
- Ideally, the preferred format they would like the information to be provided.

"Environmental Information" includes information which relates to:

- a) the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements,
- b) factors such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment referred to in (a),
- c) measures (including administrative measures), such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect the elements and factors referred to in (a) and (b) as well as measures or activities designed to protect those elements,
- d) reports on the implementation of environmental legislation,
- e) cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to in (c), and
- f) the state of human health and safety, including the contamination of the food chain, where relevant, conditions of human life, cultural sites and built structures in as much as they are, or may be affected by the state of the elements of the environment referred to in (a) or, through those elements, by any of the matters referred to in (b) and (c).

Requests for information under FOI and EIR

Any requests received should be forwarded to the SPOC who will log the request and acknowledge within five days.

The Chief Executive is responsible for:

- Deciding whether the requested information is held,
- Locating, retrieving or extracting the information,
- Considering whether any exemption or exception might apply, and the balance of the public interest test,

The SPOC is responsible for:

- Preparing the material for disclosure and drafting the response,
- Seeking any necessary approval for the response, and
- Sending the response to the requester.

FOI requests must be made in writing. NYnet will only consider requests which provide a valid name and address and NYnet will not consider requests which ask NYnet to click on electronic links. EIR requests can be made verbally, however NYnet will endeavour to follow this up in writing with the requestor to ensure accuracy.

The SPOC will consider all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. In applying the public interest test NYnet will:

- Document clearly the benefits of both disclosing or withholding the requested information,
- Where necessary seek guidance from previous case law in deciding where the balance lies,
- Consult the DPO.

Reasons for disclosing or not disclosing will be reported to the next Senior Management Team/Board meeting.

NYnet have adopted the Information Commissioner's model publication scheme and will publish as much information as possible on its website in the interests of transparency and accountability.

NYnet will charge for supplying information at its discretion, in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied.

NYnet will adhere to the required FOI and EIR timescales, and requests will be responded to within 20 working days.

Internal Reviews

Complaints in relation to FOI and EIR will be processed as an internal review request and should be made within 40 working days from the applicant receiving the original response. After that time NYnet are not obliged to respond to the request for a review.

An internal review will be dealt with by an appropriate member of staff who did not have any involvement in the original request. They will examine the original request and the response that was sent and decide whether it was dealt with appropriately, according to legislative requirements. The reviewing officer will also decide whether to uphold or overturn the decisions to withhold information. A full response will be provided within 20 working days.

If an individual remains dissatisfied after NYnet have concluded its internal review they may appeal to the Information Commissioner's Office. Their contact details are below:

Phone: 0303 123 1113 or via their live chat. Their normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on [Contact us | ICO](#).

Copyright

NYnet will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However, it will be the enquirer's responsibility to ensure that any information provided by NYnet is not re-used in a way which infringes those interests, whether or not any such warning has been given.

Appendix Four – Surveillance Policy

Introduction

This policy concerns our use of surveillance technology and related processing of personal data. It is written in accordance with data protection and human rights legislation and relevant codes of practice.

Surveillance is the close observation or monitoring of individuals or spaces, for the purpose of influencing behaviour or protecting people. We only use surveillance in the contexts described below. We do not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

CCTV

NYnet operate Closed Circuit Television (CCTV) systems to:

- Protect NYnet's buildings and property
- Protect the health and safety of our workforce and visitors
- Deter criminal activity and support in the prevention, detection, investigation and prosecution of any crimes
- Monitor compliance with NYnet's policies and procedures.

Vehicle Tracking

NYnet operate Vehicle Tracking systems to:

- Protect NYnet's vehicles
- Protect the safety of our company vehicle users
- Comply with insurance and lease requirements
- Assist with the effective management of services (via vehicle tracking and route planning etc)
- Monitor driving attributes and behaviour (such as speeding)
- Monitor compliance with NYnet's policies and procedures.

Door Access Control Data

NYnet operate Door Access Control systems to:

- Protect NYnet's buildings and property
- Protect the health and safety of our workforce and visitors
- Deter criminal activity and support in the prevention, detection, investigation and prosecution of any crimes
- Monitor compliance with NYnet's policies and procedures
- Monitor staff attendance and punctuality (where necessary).

Privacy Risk Assessment

Under the UK GDPR, we are required to consider and address privacy implications to data subjects when implementing new data processing systems. This is known as privacy by design. The usual method for assessing privacy risks to individuals is by carrying out a Data Protection Impact Assessment (DPIA).

A DPIA is mandatory for surveillance activities since they are deemed particularly intrusive. We will ensure that DPIAs have been completed for all relevant surveillance activities undertaken by NYnet and that there are no unmitigated high risks to the rights and freedoms of data subjects. In addition, we will review and update the relevant DPIA if we substantively change our systems.

Contract Management

We are required to have contracts with any data processors we use, containing certain data processing clauses prescribed by law. Where we have a direct relationship with the providers of any surveillance systems we use, we will ensure that we have implemented an appropriate contract with those providers to allow for them storing, monitoring or accessing the data on our behalf. We will

only agree to these contracts where they have been assessed for compliance and determined to meet our requirements.

Where surveillance systems are provided or managed by a third-party Data Controller (such as the Council), they will be responsible for ensuring appropriate arrangements are in place. This is to ensure the processing of information is compliant with the relevant legislation.

Transparency

The use of CCTV systems must be visibly signed. Signage will include the purpose of the system, the name of the organisation operating the system and details of who to contact about the system. The signage will be clear and kept unobstructed, so that anyone entering the area will be aware that they are being recorded.

More detailed information about our surveillance activities will also be provided via a Privacy Notice, which must also inform data subjects about their rights in relation to their surveillance data. We have included the mandatory privacy information to data subjects in our relevant privacy notices.

Access Controls

Surveillance system data will only be accessed to comply with the specified purpose.

Each system will have proportionate access controls and a nominated Information Asset Owner (IAO) who will be responsible for the governance and security of the system. The IAO may authorise other specified staff members to access data held on the systems routinely or on an ad-hoc basis.

Disclosures

A request by an individual for surveillance data held about them will be treated as a subject access request (SAR). For more information on data subjects' right of access to their information, please refer to our Data Protection Policy.

If we receive a request for surveillance data from an official agency, such as the police, then we will confirm the purpose of the request and their lawful basis for accessing the data. We may also require formal documentation in support of the request. We will liaise with our Data Protection Officer (DPO) if we have any concerns about such requests.

Record of Processing and Retention

We have a duty under Article 30 of the UK GDPR to ensure that all our data processing activities are recorded for accountability purposes. We maintain an Information Asset Register to fulfil this requirement. We will ensure that the use of surveillance systems is detailed on this register.

Surveillance records will only be held as long as necessary to fulfil the specific purpose and deleted in line with our Documents and Records Retention Policy.

Reviews

Surveillance systems must be reviewed annually to ensure that systems still comply with data protection legislation and national standards.

It is the responsibility of the relevant IAO to ensure reviews are completed and evidence of this is maintained.

Complaints

Complaints by individuals about the use of surveillance systems or data will be treated as a data protection concern. For more information on data protection complaints, refer to our main Data Protection Policy.