



General Data Protection Regulation: Responding to Personal Data Breaches

1. When there is a personal data breach, the Information Commissioner's Office (ICO) advises:

Tell it all. Tell it fast. Tell the truth.

2. The designated Data Protection Lead is responsible for handling personal data breaches. In particular, he or she will evaluate what the breach is and how it occurred, and the associated risk to data subjects and the company.
3. Senior management is committed to supporting the Data Protection Lead in response to any breach, whatever the level of seriousness.
4. If there is a risk to data subjects, the breach will be reported to the ICO within 72 hours. If the report is late, an explanation will be given as to why.
5. Where the risk to data subjects is high, the breach will be reported to them individually where possible. If there are a large number of data subjects at risk, it may not be logistically possible to do so, in which case a press release will be considered, and notification provided on the company's website, for example.
6. Encryption of personal data is likely to reduce the risk to data subjects following a breach significantly. This company encrypts high-risk personal data such as identification records, financial information and health and medical records.

7. The ICO will be told how the breach occurred, what steps are being taken to reduce the risk, and how a similar breach is to be avoided in future. The initial report will contain no more than a summary of the position. The Data Protection Lead may seek authority to obtain legal advice before submitting the initial and any subsequent reports.
8. A thorough investigation and corrective action will be taken to reduce the risks to data subjects arising out of the breach, and to ensure that something similar does not happen again in future.
9. Where a breach of the company's computer systems is suspected, to identify the breach and advise on corrective measures, the Data Protection Lead will seek support from the company's IT provider: Plan-IT Consulting Limited
10. This company has cyber security insurance and any IT-related breaches must be reported to insurers immediately. They may provide affected data subjects with free access to security measures to protect their identity.
11. The theft of data, whether as a result of shortcomings in the physical security arrangements on the premises, the hacking and penetration of computer systems, or theft by a member of staff, will be reported immediately to the police.
12. The breach, investigation and corrective actions will be documented and filed on the data protection risk register. So, too, should reports made to the ICO.
13. All personal data breaches, however minor, and whether reportable or not, such as non-compliance with the company's clear desk policy, will be recorded in the data protection risk register, held by the Data Protection Lead.



GENERAL DATA PROTECTION REGULATION: PRIVACY NOTICE

This privacy notice provides information about the personal information we process about you, in compliance with the General Data Protection Regulation (GDPR).

1. Nationwide Metal Recycling Limited is a metal and waste recycling business at the following addresses:

Head Office: Martells Quarry, Slough Lane, Ardleigh, Essex, CO7 7RU and the following sub depots: **Cambridge Depot**, Barnwell Junction, Swann Road, Cambridge, Cambridgeshire, CB5 8JZ. **Eye Depot**, The Yard, Denham Street, Nr Eye, Suffolk, IP21 5EX. **Hats Depot**, 16 Commerce Way, Whitehall Industrial Estate, Colchester, Essex, CO2 8HW. **Hitchin Depot**, Bridge Works, Cadwell Lane, Hitchin, Hertfordshire, SG4 0SA. **Holbeach Depot**, 5A Fen Road, Holbeach, Spalding, Lincolnshire, PE12 8QA

2. Our ICO registration number is Z323472X
3. Please contact Sheila Edwards using the email address:
sheila@nmrecycling.co.uk with any questions or requests about your personal information.
4. **Your rights:** We are committed to protecting your rights to privacy. They include the right to:
 - Be informed about what we do with your personal data.
 - Have a copy of all the personal information we process about you.
 - Rectification of any inaccurate or incomplete data.
 - Be forgotten and your personal data destroyed.
 - Restrict the processing of your personal data.
 - Object to the processing we carry out based on our legitimate interest.

5. The personal data we process, why we process it and how long we keep it for: As a scrap metal dealer, we are required by legislation to keep certain records for three years. These records may contain personal data and include:

- Names and addresses of suppliers of scrap metal and others we transfer metal on to.
- Verification of names and addresses such as copy driving licences, passports and utilities bills.
- Cheques and receipts confirming electronic transfers.
- Vehicle registration numbers.

6. Legitimate interests: We also process the following information because it is in our legitimate interests as a business buying and selling scrap metal to do so:

- CCTV footage (retained for one month unless it is needed for the investigation of a crime).
- Scrap metal dealer licence numbers, including documents related to our own licence (retained for 3 years).
- Waste carrier registration numbers and any documentation related to our own licence (retained for 3 years).
- Associated environmental permitting and waste shipment information (retained for 3 years).
- Invoices, receipts and accounts (retained for 6 years).
- VAT and tax returns (retained for 6 years).

Employee data: As an employer, we process personal data pursuant to contracts of employment with our employees and retain this information for six years. The information includes:

- Names, addresses and contact details. This may include next of kin details.
- Pay and bank details.
- Curricula vitae, contracts of employment and appraisals, references.
- Health information with the employee's explicit consent, which may be withdrawn at any time.

- 7. Sharing Personal data:** We share personal data internally strictly on a need-to-know basis. Access to identity records and personnel files is limited to designated individuals. Hard copy documents are stored securely. Where these documents are stored electronically, they are protected and/or encrypted. We do not share personal data with anyone external to the organisation, other than:
- Our professional advisers.
 - Police services (in connection with the investigation or detection of crime).
 - Local authorities, Environment Agency, HMRC or VAT Commissioner (where required by law).
 - Pursuant to a court order.
- 8. Information Commissioner's Office:** If you have any concerns about the way your personal information has been processed, you may contact the Information Commissioner's Office on 0303 123 1113.



General Data Protection Regulation: Data Protection Policy

1. This data protection policy is designed to ensure that the rights to privacy of individuals are protected.

Nationwide Metal Recycling Limited is committed to the principles set out in the General Data Protection Regulation and has reviewed its personal data processing activities so as to carry on its business as a scrap metal dealer in compliance with the provisions of the Regulation.

2. **Data protection lead:** This person is responsible for ensuring compliance with policies and procedures on data protection, for providing staff training, for conducting audits, risk assessments and data protection impact assessments, for responding to requests from data subjects and dealing with data breaches. He or she also handles queries and complaints from data subjects about the processing of their data, including from members of staff.

The name of the data protection lead is: Sheila Edwards

3. **Data subject:** An individual whose personal data is processed. The company processes personal data belonging to suppliers, customers, contractors, and employees.

4. **Personal data:** Any information from which a living individual can be identified, either directly or indirectly. It is not limited to names and identification numbers, or to photographs or addresses. The categories of personal data the company processes include:

- Banking details of suppliers, customers and members of staff.
- Invoices and copy receipts, copy cheques and BACS payments receipts.
- Copy passports, driving licenses, utility bills and other documents used to check identity.
- Vehicle registration numbers.
- Accounts, tax, VAT returns and related information.
- CCTV footage.
- Names, addresses, personal email addresses and telephone numbers of members of staff.
- CVs, contracts of employment, references, appraisals and salaries of members of staff.

5. **Special category data:** This is information revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic and biometric data, health information and data in relation to a person's sex or sexual orientation. The special category personal data the company holds includes:
 - Medical and other health records

6. **Processing:** Covers any activity involving personal data, including holding, storage and destruction. The Information Commissioner says it is difficult to image an activity involving personal data that does not fall within the definition. The company processes personal data during business transactions concerning the purchase and sale of scrap metal and other materials, and when carrying out other functions necessary to its business.

7. **Data processing activities include:** Filming through CCTV cameras, taking copies of identity documents and storing them in files or online, sending and receiving emails internally and externally, submitting invoices and filing them with receipts, uploading documents onto the cloud, using a customer relationship management system, holding staff details on hard copy/electronic personnel files, archiving and destroying material.

Sharing of personal data: The company shares personal data internally, and externally only when necessary to achieve its business purposes. There is no transfer of data abroad. In particular, the company shares data with the following types of organisation:

- Photocopying companies
- Confidential waste disposal companies
- Digital typing services
- Website providers
- Cloud storage providers
- IT support providers
- Accountants and other professional advisers
- HMRC
- VAT Commissioner
- Companies House.

8. **Data controller:** Decides the why and the how of personal data processing. A controller can be a sole trader, a partnership, a private or public limited company or a large multi-national organization. It decides why it needs to collect personal data and how to process it.
9. **Data processor:** Processes personal data in accordance with the written instructions of the data controller. Most of the organisations that the company shares personal data with are processors.
10. **Legitimising conditions:** The processing of personal data is unlawful unless a legitimising condition, or lawful basis, applies. The company generally relies on the following legitimising conditions:
 - Contract (with employees)
 - Legislation (in relation to ID and recording requirements, and data on the waste collected)
 - Legitimate interest as a business.

When processing special category data. The company generally relies on one of the following additional legitimising conditions:

- Legal claims
- Explicit consent

The company tries to avoid relying on the consent basis where possible. In order to be valid, consent must be freely given, and as easily withdrawn as it was to give it.

11. **Data protection principles:** Where there is a lawful basis for processing personal data, the company must make sure it carries out its personal data processing activities in accordance with various conditions or principles contained in the GDPR.
12. **Accountability:** This principle is designed to ensure that data protection is embedded in an organisation at all levels of decision making and becomes fundamental to its culture. Not only must the company comply with the General Data Protection Regulation, but it must be able to show it complies.

It is for this reason that this policy, and the appended policies have been written. All staff must receive training in these policies and managers ensure that they are implemented.

13. **Data protection by design:** This is an aspect of the accountability principle. It means that data protection risks are evaluated and eradicated and reduced at the very earliest stage, whenever there is a significant change in processes or procedures which entail a risk to data subjects. Examples: a substantial upgrade to an IT system, the introduction of CCTV cameras, outsourcing such as engaging a new cloud provider. Data Protection Impact Assessments are carried out by the data protection lead in these circumstances.
14. **Data protection by default - minimisation:** In short, no more data should be collected, shared and stored than is strictly necessary. The retention periods for the personal data the company stores are appended to this policy.
15. **Security:** This is one of the most important principles. The company must take physical, organisational and technical measures to ensure that its personal data is secure. Hard copy as well as electronic data must be processed in accordance with the company's security policy. It is important that all members of staff comply with the security policy. Failure to do so is a disciplinary offence that may result in dismissal.
16. **Personal data breach:** The Data Protection Lead is responsible for responding to personal data breaches. They must notify the Information Commissioner as necessary, and data subjects when the risk to them is high. Breaches that carry any risk to data subjects must be reported to the Information Commissioner's Office (ICO) within 72 hours, together with a summary of the nature of the breach, the steps taken, and to be taken, to reduce the risk to data subjects, as well as the measures to prevent the breach from happening again.

All personal data breaches should be recorded, whether they are reportable to the ICO or not. A data breach policy is attached.

17. **Rights of data subjects:** Data subjects have eight rights, which include:
 - Right of access to personal data by means of a subject access request.
 - Right to rectification of inaccurate data.

- Right to erasure, otherwise known as the right to be forgotten in some circumstances.
- Right to object to processing.

The company must respond to requests from data subjects within one month. The procedure for responding to requests is appended to this policy.

18. **Human Resources:** Is responsible for processing the personal data of members of staff. Hard copy files must be stored securely while electronic files must be stored securely whether they are on a computer, server or in the cloud. Access to these files should be restricted. Special category data, such as medical records, should be further restricted using encryption. No personal data should be shared outside Human Resources, except with the member of staff's manager.
19. **Data Protection Risk Register:** All personal data processing activities are recorded in the data protection risk register held by the Data Protection Lead. The risk register contains a copy of all audits, risk assessments and Data Protection Impact Assessments.
20. **Enforcement and disciplinary action:** Failure to comply with the General Data Protection Regulation is a criminal offence in many cases and can result in large fines. It is important that all staff are aware of this policy, receive training in data protection, and that this policy is properly implemented. Any staff failure to comply with this and its associated policies is a disciplinary offence, which may lead to disciplinary action and dismissal.



General Data Protection Regulation: Security Policy

This security policy is designed to ensure that Nationwide Metal Recycling Limited complies with the security requirements of the General Data Protection Regulation (GDPR), and the rights to privacy of data subjects are protected.

1. In compliance with Article 32, the company has implemented appropriate physical, organisational and technical measures to ensure a level of security appropriate to the risk.
2. The company is based at **Head Office**: Martells Quarry, Slough Lane, Ardleigh, Essex, CO7 7RU and the following sub depots: **Cambridge Depot**, Barnwell Junction, Swann Road, Cambridge, Cambridgeshire, CB5 8JZ. **Eye Depot**, The Yard, Denham Street, Nr Eye, Suffolk, IP21 5EX. **Hats Depot**, 16 Commerce Way, Whitehall Industrial Estate, Colchester, Essex, CO2 8HW. **Hitchin Depot**, Bridge Works, Cadwell Lane, Hitchin, Hertfordshire, SG4 0SA. **Holbeach Depot**, 5A Fen Road, Holbeach, Spalding, Lincolnshire, PE12 8QA.
3. The premises can be described as: Metal and Waste Recycling Company. It employs 82 staff.
4. **Physical security measures:**
 - Office building is alarmed/protected by CCTV cameras.
 - Visitors to premises are supervised at all times.
 - Areas of the premises where personal data are kept are secured by locks/complex security codes.
 - Computer screens are arranged so that they cannot be viewed by casual passers-by, particularly visitors.
 - Hard copy material containing personal data is stored securely and locked away in fire proof filing cabinets at night.
 - A clear desk policy is enforced.

- Hard copy special category data, such as medical records, are kept separately from other personal data in locked and fire proof filing cabinets, with restricted access.
- Where this information is stored electronically, it is encrypted with restricted access.
- Passports, driving licenses and any other documents used to check identity are also kept separately, stored securely with restricted access. Where stored electronically, the information is encrypted with restricted access.
- Electronic data is backed up off site.
- Any server on the premises is kept in a locked room.
- Shredding of confidential information is carried out securely on site or outsourced pursuant to a GDPR-compliant contract.
- Mobile equipment such as laptops are encrypted and locked away when not in use. There is a system in place for issuing them to staff working off site.
- Staff working off site must follow guidelines on the printing and disposal of hard copy material.
- Computers and other electronic equipment are disposed of in a safe manner by an outsourced and certificated provider.

5. Managerial security measures:

- This policy is regularly reviewed, and senior management is committed to ensuring it is implemented.
- Senior manager with responsibility for data protection ensures Data Protection Lead has sufficient resources to carry out its role effectively.
- Senior manager has powers to discipline staff for breaches of this and other data protection policies.
- Staff are trained in data protection.
- Only designated staff may delete data and they receive specific training in this regard.
- Staff compliance with this policy is monitored by file handling audits and spot checks.
- There is a procedure in place for authenticating the identity of telephone callers, customers and contractors engaged by the company.

6. Technical security measures:

- Anti-virus and anti-spyware tools are installed on all computers.
- All computers are encrypted, and password protected.
- It is a disciplinary offence to share a password.
- Computers are programmed to download patches automatically.
- Computers have automatic locking mechanisms when not in use.
- Staff are prevented from downloading software from the internet onto work computers.
- They cannot transfer data onto removable devices such as USB sticks and CDs without the authority of the Data Protection Lead.
- USB sticks and CDs used to transfer information are encrypted.
- Staff are encouraged to save personal data on their computers in a consistent manner.
- They have access rights to personal data on a strict need to know basis.
- Access rights are monitored and reviewed. They are deleted when a member of staff leaves.
- Staff are forbidden to use their personal email addresses for work.
- Personal data are encrypted before uploading onto the cloud.
- Personal data shared by email are encrypted and password protected as appropriate.

7. Security measures are reviewed, tested and evaluated at least once a year.

8. Whenever a new project, process or procedure is introduced that carries a high risk to data subjects, a Data Protection Impact Assessment is carried out, at the instigation of the Data Protection Lead.



General Data Protection Regulation: Subject Access Request

1. The rights of data subjects include the:
 - Right of access to personal data by means of a subject access request.
 - Right to rectification of inaccurate data.
 - Right to erasure, otherwise known as the right to be forgotten.
 - Right to object to processing.
 - Right to restriction on processing.

2. To respond to requests in a timely manner Nationwide Metal Recycling Limited recognises the importance of a centralised, efficient information management system. It is reviewing how it organises and stores emails and texts to enable easy and efficient retrieval. It is also reviewing the retention and storage of CCTV footage.

3. Nationwide Metal Recycling Limited stores data in relation to each customer, whether it be an organisation or individual, on a single hardcopy and/or single electronic file dedicated to the customer. The file contains evidence of all business transactions including banking details, invoices and receipts, copy cheques, BACS payment receipts, and identification records. Relevant emails, letters and faxes are also stored on these files.

4. Identification records and financial details are kept in a separate sub folder, distinct from the main file, whether the data is in hard copy or kept electronically. Hard copy files are stored in locked cabinets with access restricted to a need-to-know basis. Electronic identification records and financial details are encrypted, with similarly restricted access.

5. Records relating to employees are kept in individual files, with any medical or health related information separated into a subfolder. Hard copy files are kept in locked cabinets with restricted access. Electronic files also have restricted access and any medical or health data is encrypted.

6. The designated Data Protection Lead is responsible for responding to requests from data subjects and must do so within one month. The period may be extended by a further two months where that is necessary. In these circumstances the data subject will be informed within one month that more time is needed and the reason why.
7. Requests need not be in writing. There is no standard wording and they may be made casually over the telephone. On receipt of a request, the Data Protection Lead will log it in the data protection risk register.
8. He or she may seek to obtain the data subject's agreement to limit the request to what is being sought. Otherwise, all the data subject's personal data is covered and, in response to a subject access request, will be provided.
9. On receipt of a request, the Data Protection Lead will inform his or her manager and conduct a search of the relevant files, email folders and inboxes as necessary, as well as CCTV footage if applicable. (Given how broad the definition of personal data and processing are, reference will be made to the data protection policy for the definitions.)
10. Where a request for a copy of personal data is made electronically, it will be provided electronically.
11. If the Data Protection Lead does not wish to accede to a request, he or she will seek legal advice, with the consent of his or her manager.