

City Gateway

Data Protection Policy

Reviewed by (name)	Date	Next review needed
Diane Betts	February 2022	February 2023

This policy will be reviewed on an annual basis

Data Protection Policy

City Gateway is committed to working in accordance with the General Data Protection Regulation and with the highest standards of ethical conduct.

This policy outlines the rules, behaviours and standards required of the organisation, employees, workers and third parties working on behalf of City Gateway in relation to the collection, retention, transfer, disclosure, use and destruction of any personal data, this includes data received from third parties (such as our customers) for which City Gateway is acting as Data Processor. All workers will be responsible for data protection and must abide by the rules and policies of City Gateway.

Personal Data and Sensitive Personal Data

There are two types of personal data that fall under the GDPR and for which City Gateway, its employees, workers and third parties are responsible for. These are:

Personal Data

This is defined as any information relating to an identified or identifiable natural person. Identification can be by means of "an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." This will include IP addresses and cookie strings.

Sensitive Personal Data

Sensitive personal data includes data relating to genetic and biometric data as well as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or a person's sex life, sexual orientation or criminal offences.

Data Protection Principles

The Organisation is committed to adhering to the Data Protection Principles which state:

- Data must be processed lawfully, fairly and in a transparent manner.
- Data must be obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data processed must be adequate, relevant and limited to what is necessary.
- Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure data that are inaccurate, are erased or rectified without delay.
- Data must not be kept for longer than is necessary for the purposes for which the data are processed.
- Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

Information is kept and processed about individuals for legal purposes (such as for payroll), for administration purposes and for the purposes of day-to-day people management. City Gateway is aware that in order to process personal data, or sensitive personal data, City Gateway must rely on the data being:

- necessary for the performance of a contract, or
- in preparation for a contract, or
- to comply with our legal obligations, or
- for our legitimate business interests or
- to perform a task carried out in the public interest or in the exercise of an official authority.

If City Gateway wish to hold and process data which does not fall within conditions listed above, then we will seek to obtain the consent of the individual.

If it is necessary to obtain consent then City Gateway will write to the individual to ask for consent, ensuring that the consent is:

- Freely given, specific, informed, and unambiguous.
- Separate from other terms.
- Clear and in plain language.
- As easy to give as to withdraw.
- 'Explicit' for sensitive data.
- Given in a way that can be evidenced.

Unless consent to processing data is critical to the performance of a contract, the performance of a contract will not be made conditional on the basis that consent is given.

Employees Guidelines to Data Protection

At City Gateway we are committed to upholding the highest standards of data protection, to protect our business and keeping this information secure is the responsibility of all employees.

Employees are expected to keep a clean desk policy (whether at the office or at home), ensuring that documents are not publicly available, and that any personal data is kept securely in a locked location.

Personal and City Gateway devices used for work purposes, such as laptops, telephones, memory sticks etc must be kept with you at all times when you are not working in the office and should not leave your sight. Alternatively, they should be locked away securely, e.g., laptops stored in boot of car, locked drawer/cupboard.

Protect any personal data and sensitive personal data you are handling. If the document contains any personal information, passwords should be used. For any sensitive personal information, the documents should be encrypted prior to sending.

Whenever you are leaving your desk ensure that you press CTRL-ALT-Delete to activate a password protected screensaver.

Employees should never discuss confidential matters relating to either City Gateway or our customers in a public place, such as on trains.

You must use passwords containing a mix of upper and lower-case letters and numbers. Never share your passwords and change them regularly. Access will be cancelled if an employee leaves or is absent from the business for longer than 4 consecutive weeks. If any personal data is posted, it should always be sent by recorded delivery to ensure safe delivery.

Do not store any files or data on your computer desktop or allow any downloaded documents to be saved on to your personal devices e.g., phones, tablets. If these are accidentally downloaded/saved, they should be deleted as soon as possible.

Personal Data

City Gateway collects and processes the following personal data (this is not an exhaustive list):

- Employee/worker data, such as: names, job titles, addresses, contact details, bank details, NI.
- NI numbers, date of birth, health/medical information, next of kin details etc...
- Personal data from Data Controllers (such as customers and customers) for whom we are acting as Data Processor, such as employee names, addresses, data related to remuneration, NI numbers, date of birth, health/medical information and so on.
- Personal data from third parties as individuals for the purposes of direct marketing, including names, job titles, addresses, contact details etc.

Rights of Data Subjects

City Gateway will recognise that individuals have the following rights under data protection legislation:

- the right to be informed, which encompasses the obligation on employers to provide transparency as to how personal data will be used.
- the right of access.
- the right to rectification of data that is inaccurate or incomplete.
- the right to be forgotten under certain circumstances.
- the right to block or suppress processing of personal data; and
- the new right to data portability which allows employees to obtain and reuse their personal data for their own purposes across different services under certain circumstances.

Right of Access

Individuals have the right to access the information stored about them and can ask for access to their own personal details held electronically or held manually. Individuals who wish to see their records should give notice electronically, in writing, using a Subject Access Request Form which is available upon request. City Gateway has up to 1 month to provide the information following the subject access request, which it will usually do in electronic format.

In complex cases, or where there are numerous related requests, City Gateway will liaise with the individual to inform them of progress of their request(s), and if it is not possible to complete this within 1 month, City Gateway will inform the individual of the delay, the reasons for the delay and reserves the right to extend the timescale for completion by up to a further 2 months.

In the event that data is retained with third parties, City Gateway will ensure that the request is communicated and actioned by the third party in line with the timescales outlined above, unless impossible or if it would require disproportionate effort.

City Gateway reserves the right to charge a fee or to refuse to respond to a request if it is manifestly unfounded or excessive. Similarly, City Gateway reserves the right to withhold personal data if disclosing it would adversely affect the rights and freedoms of others.

Rectification of Data

City Gateway is committed to keeping data that is accurate and up to date. Data will be checked for accuracy where possible, and any data that is inaccurate, out of date or unnecessary will be corrected or erased as appropriate.

Where an individual identifies that their personal data is incorrect or incomplete, or where they are aware that their personal data has changed, they must inform the organisation as soon as possible. The organisation will then take steps to rectify any inaccuracies as soon as possible, and at the latest within 1 month.

In complex cases, or where there are numerous cases, City Gateway will liaise with the individual to inform them of progress of their request, and if it is not possible to complete this within 1 month, City Gateway will inform the individual of the delay and the reasons for the delay and reserves the right to extend the timescale for completion by up to a further 2 months.

In the event that data has been disclosed to third parties, City Gateway will ensure that the request for rectification is communicated and actioned by the third party in line with the timescales outlined above, unless this is impossible or if it would involve disproportionate effort.

The Right to be Forgotten

Also known as 'the right to erasure', the right to be forgotten doesn't provide an absolute right to be forgotten, but individuals have a right to have personal data erased and to prevent processing in some circumstances i.e.

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed.
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

If an individual wants to ask for their own personal data to be partially/fully erased and no longer processed, please write to the CEO with full details of your request. City Gateway has up to 1 month to respond to you and either delete the data or explain why it is unable to comply with your request. Circumstances where City Gateway may be unable to comply include where it is required to retain the information by law, or if the data is needed in connection with legal proceedings.

In complex cases, or where there are numerous related requests, City Gateway will liaise with the individual to inform them of progress, and if it is not possible to respond to this within 1 month, City Gateway will inform the individual of the delay, the reasons for the delay and reserves the right to extend the timescale for completion by up to a further 2 months, if necessary.

In the event that data is retained with third parties, City Gateway will ensure that the request is communicated and if appropriate actioned by the third party in line with the timescales outlined above.

Security of Data

City Gateway is committed to taking steps to ensure that personal data is protected, and to prevent any unauthorised access, accidental loss, destruction, unlawful processing, equipment failure or human error, and will do this through the continual monitoring of our security systems and by regular training and awareness raising.

Any data breaches will be managed according to the procedures documented in our Data Protection Breach Reporting Policy and Procedure.

Data Retention

City Gateway is committed to ensuring that personal data is kept for no longer than necessary and only kept as long as it's relevant and necessary for legitimate purposes. As soon as data is no longer necessary for the purposes for which it was originally collected, it will be securely deleted, unless it is necessary to keep the data for some other legitimate reason.

City Gateway does not intentionally keep data longer than necessary and when data is no longer required, City Gateway is committed to securely deleting it as soon as possible. For more information and our retention guidelines, please refer to our Data Retention Policy.

Data Breaches

All staff are responsible for data protection and should be alert to any actual, suspected, threatened or potential data protection breaches. As soon as a data protection breach has been discovered, where possible, the member of staff should complete a Data Protection Breach Reporting Form (to the fullest extent possible at that time), which provides full details concerning the breach. This form should then be passed to CEO as soon as possible and within 24 hours of the discovery of the breach. If you need help completing the form, or are unable to complete the form, then any delay should be avoided and instead the matter should be reported immediately at least within 24 hours, either verbally or using electronic means, such as email.

For more information regarding managing data protection breaches, please refer to the Data Protection Breach Reporting Policy and Procedure.

Objections to Personal Data Processing

You have the right to object to data processing when City Gateway is:

- processing information based on its legitimate business interests, or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing
- processing for the purposes of scientific/historical research and statistics.

If you wish to object to processing, you should write to the CEO outlining the grounds relating to your particular situation and City Gateway will stop the processing unless it has compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is in relation to legal claims. If City Gateway is unable to agree to your request, you will be written to and the reason why will be explained, along with your right to complain to the ICO.

Data Protection Measures

City Gateway is committed to ensuring the security of your data and to processing it in line with the Data Protection rules. As such, City Gateway will:

- Ensure that all staff are aware of their responsibilities and City Gateway's obligations and responsibilities in relation to data protection.
- Ensure that all staff are aware of and adhere to City Gateway's Information Security Guidelines.
- Ensure that all staff who handle data on behalf of City Gateway are appropriately trained and receive refresher training on a regular basis.
- Ensure that all staff and Data Processors who handle data on our behalf are regularly monitored, assessed and reviewed.
- Ensure that all of the Data Processors working on behalf of City Gateway who handle data on our behalf are carrying out data processing in line with the Data Protection rules.
- Regularly audit and work to continuously improve City Gateway's methods of data collection, handling, processing and storage.

Monitoring

We are committed to monitoring this policy and will update it as appropriate, on an annual basis or more frequently if necessary.

Data Retention Policy

City Gateway is committed to managing and handling personal data in line with best practice and data protection principles. As such this Policy details the procedures to use to ensure timely and secure disposal of documents and records that are no longer required for business purposes.

City Gateway holds a wide variety of personal data, from employees, workers, and contractors, as well as financial data, customer data. This data is held in various formats including, letters, emails, contracts, forms, software systems in both hard copy and electronic form.

It is essential that this policy is adhered to, as premature destruction of documents could result in an inability to defend claims, business difficulties and failure to comply with data protection legislation, whilst appropriate destruction and disposal will ensure that the storage space is maximised, and we are not keeping documents for an unnecessarily long period of time which would breach the data protection legislation.

This policy applies to all the information held by City Gateway and also any personal data that may be held by data processors (service providers) where they are processing information on City Gateway's behalf.

All employees are responsible for ensuring that the records that they create/maintain are accurate, maintained and disposed of in accordance with this policy. It is recognised that the documentation created and maintained by City Gateway will change over time and therefore this policy should be viewed as a living document and it will be reviewed on an annual basis, or as necessary, if sooner.

This policy should be read in conjunction with the Data Protection Policy and the Data Protection Breach Reporting Policy.

Destruction/Disposal

Hard copies of confidential documents or personal data should be disposed of using the confidential waste bins and sacks. Under no circumstances should any personal or confidential data be disposed of in any other manner, as this would potentially breach data protection legislation.

Disposal of documents which do not contain personal data or confidential information can be disposed of in any bin, or by recycling or by electronic deletion in the case of electronic documents.

Records of disposal should be maintained, recording the document disposed of, date and the individual responsible for authorising the disposal.

Data Protection Breach Policy and Procedure

City Gateway is committed to handling personal data in line with best practice and as such this policy details the procedures to use when dealing with and responding to data protection breaches. This is to ensure that incidents are responded to promptly, risks are minimised, learnings identified, and remedial actions are implemented.

These procedures apply to all staff, suppliers, contractors, agency workers, volunteers, customers, data processors or anyone else who may handle or have an interest in personal data on behalf of City Gateway.

Discovery

All individuals, or organisations (including Data Processors) working on behalf of City Gateway are responsible for data protection and should be alert to any actual, suspected, threatened or potential data protection breaches. As soon as a data protection breach has been discovered, where possible, a Data Protection Breach Reporting Form should be completed (to the fullest extent possible at that time), which provides full details concerning the breach. This form should then be passed to the CEO as soon as possible and within 24 hours of the discovery of the breach. If you need help completing the form, or are unable to complete the form, then any delay should be avoided and instead the matter should be reported immediately, either verbally or using electronic means, such as email.

Once a data protection breach has been reported, an initial assessment will be made by a senior manager within City Gateway concerning the content, quality of data involved and the potential impact and risk of the breach.

Reporting

Following a discovery of a breach and the receipt of such a report, consideration will be made regarding whether the matter needs to be reported to the Information Commissioner's Office (ICO) and whether individuals who are potentially affected need to be informed.

Current legislation states that any data protection breaches that are likely to result in a risk to the rights and freedoms of the individuals concerned (irrespective of their severity) must be reported to the ICO as soon as possible and no later than 72 hours after their discovery.

In addition to this, the individuals affected by the breach must be informed if the breach is likely to pose a high risk to them. The individuals must be informed of the nature of the data breach and the steps that City Gateway is taking to protect their data.

The incident will also be logged in the Data Protection Breach Register.

Containment and Recovery

As soon as possible after the discovery of an actual or suspected data protection breach, consideration will be given to:

- whether the breach has been contained as far as possible and whether any further steps can be taken to contain the data from further loss.
- whether any steps can be taken to mitigate the impact and risk of the loss.
- whether anything can be done to recover the data.

Any employees who act in breach of this policy or who do not implement it, may be subject to formal disciplinary proceedings, which may involve dismissal depending on the relevant circumstances. Any third parties or workers who act in breach of this policy or fail to implement it may have their relationships with City Gateway terminated with immediate effect.