General Data Protection Regulation Policy

Countrywide Upvc (Northwest) Limited is committed to a Policy of protecting the rights and privacy of individuals, including Management, Staff, and others, in accordance with the General Data Protection Regulation (GDPR) which came into force on 25th May 2018.

The new regulatory environment demands higher transparency and accountability in how the Company manages and use personal data. It also accords new and stronger rights for individuals to understand and control that use. The GDPR contains provisions that the the Company will need to be aware of as data controllers, including provisions intended to enhance the protection of Clients and individual's Personal data.

Compliance:

This Policy applies to all management, and staff of the Company.

Any breach of this Policy or of the Regulation itself will be considered an offence and the Company's disciplinary procedures will be invoked. As a matter of best practice, other agencies and any individuals working with the Company and who have access to Client or Personal information, will be expected to read and comply with this Policy.

It is expected that any person or department who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this Policy.

This Policy will be updated as necessary to reflect best practice in data management, and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

Data Protection Principles:

The Company is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

- Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes as required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

General Provisions:

- This Policy applies to all personal data processed by the Company.
- The Responsible Person shall take responsibility for the Company's ongoing compliance with this Policy.
- This Policy shall be reviewed at least annually.
- Lawful, fair and transparent processing

Individuals have the right to access their personal data and any such requests made to the Company shall be dealt with in a timely manner.

Lawful purposes:

All data processed by the Company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Company's records.

Technical and Organisational measures:

The Company will put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

The Company will ensure that all personal data is accessible only to those who have a valid reason for using it.

The Company will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (i.e. with the keys then held securely in a key cabinet with controlled access):

Controlled access may include:

● keeping all personal data in a lockable cabinet with key-controlled access.
● password protecting personal data held electronically.
● archiving personal data which are then kept securely (lockable cabinet).
● placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.
● ensuring that PC screens are not left unattended without a password protected screen-saver being used.

Personal Information:

Information protected under the GDPR is known as "personal data" and is defined as: - "Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Further information on what constitutes personal information and your rights under the data protection regulation and laws can be found on the Information Commissioners Office (ICO) website.

Data minimisation:

The Company shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy:

The Company shall take reasonable steps to ensure personal data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving / Removal:

To ensure that personal data is kept for no longer than necessary, the Company shall put in place an archiving Policy for each area in which personal data is processed and review this process annually. The archiving Policy shall consider what data should/must be retained, for how long, and why.

Security:

The Company shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information. When personal data is deleted this should be done safely such that the data is irrecoverable.

Appropriate back-up and disaster recovery solutions shall be in place.

Breach:

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Company shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

Procedure for review:

This Policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

Name of Responsible Person: Michael Campbell

Declaration:

Name:

Signed:

Date:

Date of Review: September 2018