WAVEPOINT GROUP

DATA PROTECTION POLICY

How we collect, use and protect personal information

Wavepoint Group Limited — How we collect, hold, use and protect personal information

Document owner	Managing Director	**Policy reference**	WPG-GOV-03
Version	2.0	**Status**	Approved
Date issued	24 June 2026	**Next review**	24 June 2027
Approved by	Jason Alexander, Managing Director	**Applies to**	All staff, workers & third parties

OUR DATA PROTECTION COMMITMENTS AT A GLANCE

Lawful & Fair | **Kept Secure** | **Individual Rights** | **Breach Response** | **Accountable & Reviewed**

1. Policy Statement

Everyone has rights regarding how their personal information is handled. Wavepoint Group Limited ("the Company", "we", "us") is committed to protecting the personal data of our employees, workers, customers, suppliers and anyone else we deal with, and to handling it lawfully, fairly and transparently.

This policy sets out our approach to data protection and the rules that must be followed when obtaining, holding, using, sharing, storing and disposing of personal information. It applies to all officers, employees, agency workers, consultants and contractors working for or engaged by the Company (together "staff"), and to third parties with access to our systems. It does not form part of any employee's contract of employment and may be amended at any time. Any breach is taken seriously and may result in disciplinary action.

2. Legal Framework

We comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, and with guidance issued by the Information Commissioner's Office (ICO). The Company is registered with the ICO and pays the data protection fee. Wavepoint Group Limited is the data controller for the personal data described in this policy.

Our Data Protection Lead is responsible for overseeing compliance with data protection law and this policy. Any questions, concerns or requests should be referred to the Data Protection Lead in the first instance.

3. Key Definitions

- Personal data — information relating to an identified or identifiable living individual (for example a name, address, email, ID number or online identifier).
- Special category data — more sensitive data such as health, racial or ethnic origin, religious or philosophical beliefs, trade union membership, sex life or sexual orientation, and biometric or genetic data, which requires extra protection.
- Data subject — the living individual the personal data is about.
- Data controller — the organisation that decides how and why personal data is processed (here, the Company).
- Data processor — a person or organisation that processes personal data on the controller's behalf (for example certain suppliers).
- Processing — any activity involving personal data, including collecting, recording, storing, using, sharing, erasing or destroying it.

4. The Data Protection Principles

Anyone processing personal data must comply with the principles of the UK GDPR. Personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not used in a way incompatible with those purposes (purpose limitation);
- adequate, relevant and limited to what is necessary (data minimisation);
- accurate and, where necessary, kept up to date;
- kept in a form that identifies individuals for no longer than necessary (storage limitation); and
- processed securely, with appropriate protection against unauthorised processing, loss, damage or destruction (integrity and confidentiality).

Underpinning these is the principle of accountability: we must be able to demonstrate our compliance with the above.

5. Lawful Basis for Processing

We will only process personal data where we have a lawful basis to do so. Depending on the circumstances, this will be one or more of:

- consent of the data subject;
- performance of a contract with the data subject (or to take steps at their request before entering a contract);
- compliance with a legal obligation (for example tax, National Insurance or statutory sick pay);
- protection of someone's vital interests (a life-threatening situation);
- performance of a task in the public interest; or
- our legitimate interests (or those of a third party), where these are not overridden by the individual's rights.

Where we process special category data, we will identify an additional condition for processing, which will often require the individual's explicit consent.

6. Transparency

When we collect personal data we tell people, usually through a privacy notice, who we are, the purposes for which we will use their data, the lawful basis for doing so, how long we keep it, who we may share it with, and their rights. We will not use personal data for a new, incompatible purpose without informing the individual.

7. Individuals' Rights

Subject to certain conditions and exemptions, data subjects have the right to:

- be informed about how their data is used;
- access their personal data (a "subject access request");
- have inaccurate data rectified;
- have data erased in certain circumstances (the "right to be forgotten");
- restrict or object to processing, including for direct marketing;
- data portability; and
- rights relating to automated decision-making and profiling.

8. Subject Access and Other Requests

- Any member of staff who receives a request from an individual to exercise their rights must forward it to the Data Protection Lead immediately.
- We respond to subject access requests free of charge and within one month, which may be extended for complex or numerous requests.
- We only carry out reasonable and proportionate searches in responding to a request, and we verify the requester's identity before disclosing any information.
- We will help individuals who wish to make a complaint about how we use their data, acknowledging complaints promptly and responding without undue delay.

9. Data Security

We put in place appropriate technical and organisational measures to keep personal data secure throughout its life, protecting its confidentiality, integrity and availability. Measures include:

- access controls and reporting of any unauthorised person seen in restricted areas;
- locking desks and cupboards that hold confidential information, and keeping personal data on our central, secured systems rather than individual devices;
- secure disposal — shredding paper records and securely wiping or physically destroying electronic media;
- screen awareness and logging off unattended devices; and
- only sharing personal data with a processor where it is bound by a written contract to keep the data secure and to act on our instructions.

10. Personal Data Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. All staff must report any suspected breach to the Data Protection Lead immediately. Where a breach is likely to result in a risk to

individuals, we will report it to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it, and will inform affected individuals where the risk to them is high.

11. Sharing and International Transfers

We only share personal data where it is lawful and necessary. Where personal data is transferred outside the UK, we ensure an appropriate safeguard or transfer mechanism is in place so that the data remains adequately protected.

12. Telephone Enquiries

- Staff dealing with telephone enquiries must take care before disclosing any personal data, and check the caller is entitled to the information.
- If identity cannot be verified, ask the caller to put their request in writing.
- Refer difficult situations to the Data Protection Lead — no one should be pressured into disclosing personal information.

13. Retention and Disposal

We keep personal data only for as long as necessary for the purpose for which it was collected and in line with our retention schedule and legal obligations. Personal data is securely deleted or destroyed when it is no longer required. Where there is a realistic prospect of legal proceedings, relevant data may be retained for longer in line with limitation periods.

14. Monitoring and Review

We review the effectiveness of this policy to ensure it continues to meet its objectives and remains compliant with current law and ICO guidance. This policy is reviewed at least annually, and sooner if legislation or circumstances change.

Approved and signed on behalf of Wavepoint Group Limited

Signed	Jason Alexander
Position	Managing Director (Data Controller)
Date	24 June 2026
Review date	24 June 2027

— End of Data Protection Policy —