



ASTRAL LIMITED

**INFORMATION GOVERNANCE
POLICY**

**(DATA PROTECTION, GDPR, PRIVACY &
CYBER SECURITY)**

Reviewed: January 2026
Next Review: January 2027

Information Governance Policy
(Data Protection, GDPR, Privacy & Cyber Security)

1) Purpose & Scope

This combined policy sets out how **Astral Limited** ("Astral", "we", "us") governs, protects, and lawfully processes information—covering **personal data** (GDPR & Data Protection), **privacy** (public-facing notice content), and **information security & cyber security** (technical/organisational controls). It applies to all Astral activities, systems, and people: employees, directors, temps, contractors, and suppliers handling Astral information

2) Governance & Roles

- **Data Controller:** Astral Limited, 66 High Street, Blue Town, Sheerness, Kent, ME12 1RW.
- **Data Protection Lead (DPL):** *Adam Houghton/Director* – responsible for GDPR compliance, rights handling (SARs), and retention
- **Information Security Lead (ISL):** *Adam Houghton/Director* – responsible for cyber controls and incident response.
- **All Staff & Contractors:** must follow this policy, protect data, complete training, and report incidents immediately.

3) Principles We Follow

- **GDPR/Data Protection Principles:** lawfulness, fairness, transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity & confidentiality; accountability.
- **Information Security (CIA):** Confidentiality, Integrity, Availability of information assets.

4) What We Process & Lawful Bases

Typical personal data we process includes:

- **Employees:** contact details, NI/payroll, training records.
- **Clients/Suppliers:** contact details, addresses, payment information.
- **Communications/website data** as necessary to deliver services and manage relationships.
Lawful bases: **Contract, Legal Obligation, Legitimate Interests**, and **Consent** (where required).

5) How We Use Personal Data

To deliver projects/services, manage employees and subcontractors, meet legal/financial duties, maintain accounts, procure, and support business operations—only as necessary and proportionate to the purpose.

6) Privacy Information (Transparency)

Astral will be transparent about how we collect, use, and share personal data, keep it accurate and up to date, and secure it appropriately. Individuals can ask questions or raise concerns via our contact in Section 15.

7) Data Sharing & Processors

We share personal data with third parties **only where necessary**, under written terms requiring appropriate confidentiality and security—e.g., accountants, payroll/HR providers, insurers, IT/cloud providers, HMRC, and regulators. We assess and monitor processors' security and require breach notification

8) International Data Transfers

We do not routinely transfer personal data outside the UK. If transfer is necessary, we will use appropriate safeguards (e.g., UK IDTA/Addendum or equivalent)

9) Retention & Deletion

We retain data only as long as needed for the purpose or to meet legal obligations, then delete or anonymise it securely. Typical periods include:

Employee records: 6 years; Payroll: 6 years; Client records: 7 years; certain H&S/medical records: up to 40 years (where legally required).

10) Security Controls (Technical & Organisational)

Astral applies layered controls and user responsibilities, including:

- **Access control & passwords:** strong, unique passwords; **MFA** where available; least-privilege access; prompt leaver access removal; no shared accounts.
- **Device security:** up-to-date AV/endpoint protection; patching; auto-lock; approved use of personal devices under policy; immediate reporting of loss/theft.
- **Email/Internet:** use business email; anti-phishing vigilance; encrypted/password-protected sharing when required; approved file-sharing only.
- **Physical security:** locked offices/stores; visitor supervision; secure disposal (e.g., shredding).
- **Cloud & backups:** reputable cloud platforms with encryption; regular, tested backups; approved storage locations only; regular configuration reviews.
- **Threat protection:** firewalls; anti-malware; patching; restricted admin rights; block high-risk sites/apps.

- **Remote/mobile working:** secure Wi-Fi (or VPN on public Wi-Fi), screen privacy; minimal local downloads.
- **Training & awareness:** periodic training on cyber, phishing, data handling, and device use.

11) Individual Rights & Requests

We support rights under UK GDPR: **access, rectification, erasure, restriction, objection, portability, and withdrawal of consent** (where applicable). Requests should be directed to the DPL; proof of ID may be required. We respond within statutory timelines and record outcomes.

12) Data Protection Impact Assessments (DPIAs)

We will conduct DPIAs where processing is likely to result in high risk to individuals (e.g., new tech, large-scale monitoring, special category data) and embed appropriate measures before proceeding.

13) Breach Detection, Reporting & Response

All suspected **data/security incidents** (e.g., phishing, lost device, unauthorised access, mis-send) must be reported **immediately** to the ISL/DPL. We will investigate, contain, and record incidents; notify the ICO within **72 hours** where required and affected individuals where there is a high risk to their rights and freedoms; and implement lessons learned.

14) Supplier & Subcontractor Information Security

Suppliers/subcontractors with access to Astral systems or data must meet minimum security standards (Cyber Essentials recommended), protect personal data in line with UK GDPR, and **notify** Astral immediately of any breach affecting our data. Astral may audit or request evidence of controls

15) Contact & Complaints

Data protection & privacy contact: *Adam Houghton/Director*, Astral Ltd, 66 High Street, Blue Town, Sheerness, Kent, ME12 1RW. Individuals can also raise concerns with the UK **Information Commissioner's Office (ICO)**.

16) Training, Monitoring & Review

All staff must complete relevant training on data protection and cyber security. We monitor compliance through audits, reviews of incidents/SARs, and supplier checks. This policy is **reviewed annually** or sooner following legal, operational, or security changes.

17) Related Documents

- Acceptable Use Policy
- Cyber Security Incident Response Procedure

- Records Retention Schedule
- Whistleblowing Policy
- HR/Recruitment & Vetting Policy
- Procurement & Supplier/Subcontractor Management

18) Approval

This combined Information Governance, Data Protection, Privacy & Cyber Security Policy is approved by Astral's Managing Director and takes effect from the issue date below.



Signed:

Managing Director

Date: 05/01/2026