

PUBLIC GOVERNANCE FRAMEWORK

GDPR, PECR and Data Governance Framework

School Connection Intelligence | Schools Intelligence Observatory | Supplier-facing intelligence services

Document control	Position
Legal entity	Newscast Media Group Ltd, registered in Scotland, company SC469540
Registered office	Suite 4 Pentland House, Saltire Centre, Glenrothes, Fife, KY6 2AH
ICO registration	ZC018112
Document owner	Newscast Media Group Ltd
Version and status	Version 1.0 Public Effective 30 August 2026
Review	Review by 30 August 2027, or earlier after a material processing or legal change
Privacy contact	chris@schoolconnection.co.uk

This public framework states the controls the service must apply. It is not an ISO certification, legal opinion or substitute for engagement-specific due diligence. A control may be represented to a client only where evidence supports it for the relevant scope.

This framework should be read with the public privacy notice, cookie notice, intelligence standards and website terms at schoolconnectionintelligence.co.uk/legal.

1. Purpose and scope

This document states the data protection, electronic communications and intelligence governance controls required for the School Connection Intelligence website and supplier-facing services. It covers the Schools Intelligence Observatory, professional B2B intelligence, client-supplied programme data, enquiries, communications, expert participation and any qualified introduction arising from a defined engagement.

It is a public governance framework, not a certification. A signed client agreement, statement of work, data-sharing schedule or data processing agreement may impose more specific obligations and takes precedence for that engagement. A prospective client may request appropriate underlying evidence under confidentiality.

2. Controller and responsibility position

Newscast Media Group Ltd is the controller for personal data it collects and processes for its own website, network, intelligence, editorial and business purposes. Controller or processor roles for a client programme are determined from the actual purpose, instructions and contract rather than a generic label.

A client is usually a separate controller for its own prospect data and subsequent sales activity. A recipient of a qualified introduction usually acts as an independent controller for its later contact and must establish its own lawful basis, transparency, security, retention and suppression controls.

3. Executive operating model

- Signal: a policy, operational, estate, workforce, digital, school-published or other relevant source records a change.
- Evidence: source, date, scope, permitted use and limitation remain attached.
- Connection: the affected organisation, professional context and Connected-System effects are assessed.
- Interpretation: a human reviewer decides whether the evidence supports analysis, communication, a client output or no action.
- Control: only necessary information enters an agreed client or handover route.

4. Information categories and exclusions

Category	Examples	Control objective
Website and security	IP address, request timing, device or browser data, security events and essential cookie data.	Secure delivery, abuse prevention and operational diagnosis.
Enquiry and relationship	Name, organisation, role, business contact details, message, meeting notes and service interest.	Respond, scope, contract and administer the professional relationship.
Client programme	School names, URNs, postcodes, organisation records, agreed prospect files and solution scope.	Answer one defined client question under agreed access and retention controls.
Professional intelligence	Name, role, employer, public business contact details and relevant public professional activity.	Connect education change to responsible professional context.
Derived intelligence	Affected cohort, evidence state, priority band, role-family mapping, relevance classification and inferred operational consequence.	Organise evidence for human review; never treat a classification as proof of need, intent or authority.
Engagement and preference	Topic interest, communication history, permission route, opt-out, objection and suppression status.	Keep contact relevant and honour rights and preferences.

Most Observatory records concern organisations, schools, trusts, places, assets, policy and operating conditions rather than identifiable people. The supplier service is not designed to receive pupil-level records, safeguarding case data, health data or other special-category information about children. Clients must not provide such material.

5. Sources and provenance

- Information provided directly by an enquirer, contributor, client or authorised organisational contact.
- Official and public sources, including government, regulatory, corporate, charity, procurement, planning, school and trust publications.
- Public professional sources where the role, purpose and expected use are relevant.
- Service providers or data suppliers where provenance, permitted use and contractual safeguards have been assessed.
- Newscast Media Group's own editorial, research, correction, engagement and preference records.

Every material source category should retain its publisher, source location, acquisition and verification dates, coverage statement, transformation, licence or permitted-use basis and known limitations. Public availability is not treated as unrestricted permission for personal data.

6. Purposes and lawful bases

Purpose	Basis to apply	Safeguard
Enquiries and requested pre-contract steps	Steps at the individual's request before contract; legitimate interests for ordinary business administration.	Use remains connected to the enquiry and clearly explained follow-up.
Client delivery and contract administration	Contract where the contracting person is an individual; legitimate interests where the client is an organisation; legal obligation for specified records.	Purpose, access, output, roles and retention are defined for the engagement.
Professional education intelligence	Legitimate interests, following a purpose, necessity and balancing assessment.	Source, relevance, expectations, impact, transparency and objection are considered.
Role-relevant B2B communication	Consent where PECR requires it; otherwise legitimate interests where appropriate for corporate B2B communication.	Clear identity, relevance, valid opt-out and suppression screening.
Security and legal records	Legitimate interests and legal obligation, depending on the record.	Access, logging, minimisation and retention controls.

Legitimate interests is not automatic permission. The actual interest, necessity and balance against the individual's rights and reasonable expectations must be documented for the processing concerned.

7. PECR and subscriber classification

Corporate subscribers, including limited companies, LLPs and other corporate bodies, are treated differently from individual subscribers under PECR. A named professional remains personal data under UK GDPR even where prior PECR consent is not required for the corporate communication.

Route	Compliance position
Corporate B2B electronic mail	Sender identity must be clear, a valid opt-out address must be provided, the professional use must be fair and suppression must be respected.
Sole trader or relevant partnership	Consent or a valid limited exception is required for electronic mail marketing. Legitimate interests cannot override a PECR consent requirement.
Direct enquiry	Use is limited to the request and clearly connected follow-up. A separate marketing purpose requires its own assessment.

8. Article 14 and public-source transparency

Where identifiable professional information is obtained indirectly, the process considers Article 14 transparency, source, purpose, reasonable expectations and any applicable exception. Privacy information is normally provided within one month of obtaining the data, at first communication or before first disclosure, whichever applies first.

A disproportionate-effort exception for wider public-source monitoring must be assessed and documented rather than assumed. Appropriate safeguards and a data protection impact assessment screening are required where the scale, combination, novelty or impact may create a high risk.

9. Client files and programme controls

Before a client file is accepted, the engagement must define access, matching purpose, permitted output, security, retention, deletion and controller or processor roles. The operating rule prohibits absorbing the file into unrelated campaigns.

A priority label means current evidence warrants human attention under agreed criteria. It is not proof of buying intent, budget, purchasing authority, tender timing or a guaranteed opportunity.

10. Qualified introductions and data minimisation

Clients do not receive general access to the network or contact database. A named professional is not passed to a supplier merely because the system detects relevance or content engagement. Any identity-level supplier handover requires an affirmative request or valid consent specifically covering that follow-up. Legitimate interests may support separately assessed internal research or corporate B2B communication; it is not used to manufacture permission for a handover.

Where a qualified introduction is authorised, disclosure is limited to the organisation, necessary professional contact data, relevant location, the enquiry or engagement theme and sufficient handover context for the agreed follow-up.

Test	Required outcome
Sector, role and topic	The organisation, professional responsibility and subject align.
Permission and lawful basis	An identity-level supplier handover requires an affirmative request or valid consent. Other processing requires its own documented lawful basis.
Reasonable expectation	The contact is not surprising, intrusive or unrelated.
Opt-out and suppression	An applicable objection prevents the handover or communication.
Purpose and minimisation	Only information necessary for the agreed purpose is disclosed.

11. AI, automation and human decisions

- Automation may collect, normalise, match, deduplicate, classify, compare and monitor evidence.
- AI-generated wording is treated as assistance, not verified fact or a publication decision.
- Material client-facing claims require accessible source evidence and human review.
- Automation does not silently publish, approve a handover or make a solely automated decision about an individual with legal or similarly significant effects.

12. Editorial and audience separation

School Connection serves school and trust leaders in the public interest. School Connection Intelligence separately serves education suppliers. Commercial participation cannot purchase or direct School Connection's question, investigation, evidence, wording, publication, correction or withdrawal.

13. Security and accountability

The operating standard requires risk-based access management, minimisation, environment and audience separation, encryption in transit, processor and supplier review, change management, logging, backup and recovery, incident triage, breach assessment and contractual confidentiality. A control may be represented to a client only where evidence supports it for the relevant service and scope.

Before relevant personal-data processing or disclosure is activated, the accountability record must contain the applicable processing record, lawful-basis assessment, source and provenance record, Article 14 decision, DPIA screening, data-sharing terms, suppression approach, retention decision and human approval history.

14. Retention, rights and suppression

Information is retained only while its documented purpose, contract, legal requirement or defensible business need continues. Criteria include source recency, role change, engagement status, client instruction, limitation periods and the need to retain minimal suppression data so an objection is not forgotten.

Applicable rights include access, source information, correction, erasure, restriction and objection. Direct-marketing objections are absolute. Once received, personal data is no longer used for that purpose and only the minimum suppression information is retained as necessary.

15. Complaints and incident route

Data protection complaints may be sent to chris@schoolconnection.co.uk with the subject 'Data protection complaint'. Newscast Media Group Ltd will acknowledge receipt within 30 days, investigate appropriately, keep the complainant informed and communicate the outcome without undue delay. Individuals may also complain to the Information Commissioner's Office.

16. Client due diligence and contractual controls

Before personal information is disclosed or used in a managed communication, the purpose, audience, permitted use, security, retention, opt-out handling and onward-disclosure restrictions must be reviewed. Client terms must prohibit resale, unrelated reuse, undisclosed onward transfer and indefinite retention.

For a material engagement, an appropriate confidential assurance pack can address processing roles, lawful basis, Article 14, security, retention, suppression, incident terms and relevant processor information. Contractual assurance does not expand unsupported public claims.

17. Evidence limitations

An intelligence signal is not proof of need, available budget, purchasing authority, tender timing, supplier eligibility, buying intent, a sales-ready lead, a future contract or a commercial outcome.

18. Reference points

- Information Commissioner's Office: right to be informed, legitimate interests, B2B marketing, individual rights and DPIA guidance.
- Data Protection Act 2018 and UK GDPR.
- Privacy and Electronic Communications (EC Directive) Regulations 2003, as amended.
- School Connection Intelligence public privacy, cookies, intelligence standards, terms and data complaints documents.

END OF PUBLIC FRAMEWORK

For a compliance review, contact chris@schoolconnection.co.uk.