PARTNER & SUPPLIER ASSURANCE PACK

Version 4.0 - April 2026

WEBSITE:

cyber-rebels.co.uk

PHONE:

07473 256429

EMAIL:

hello@cyber-rebels.co.uk

Cyber Rebels Ltd Assurance Pack

Procurement reassurance and due diligence support
Updated to align with the current Cyber Rebels operating system and trust standards

Purpose of this pack
This document is intended to support supplier assurance, procurement review, safeguarding checks, and late-stage due diligence. It summarises how Cyber Rebels delivers training safely, handles data responsibly, and maintains the operational, governance, and compliance controls that partner organisations commonly need to review.

Key assurance details

Legal entity	Cyber Rebels Ltd
Primary service	Live, instructor-led cybersecurity and digital safety training for organisations, schools, youth settings, and community groups
Delivery model	Remote and on-site delivery, tailored to audience, safeguarding requirements, and operating environment
ICO registration	ZB892477
UKPRN	10098239
Insurance cover	Public Liability £2,000,000 I Professional Indemnity £1,000,000 I Cyber Insurance £1,000,000
Policy hub	https://cyber-rebels.co.uk/our-policies-and-terms

1. About Cyber Rebels

Cyber Rebels Ltd is a specialist training organisation providing live, interactive cybersecurity and digital safety education. The organisation works with businesses, schools, youth organisations, and community groups, with delivery adapted to the environment, audience, and safeguarding context of each engagement.

Its work is grounded in a clear view of cyber risk: incidents are rarely caused by a lack of information alone. More often, they arise during ordinary work, when people are making decisions under pressure, within familiar systems, and inside day-to-day routines. Cyber Rebels training is

designed to help people recognise those moments, apply proportionate judgement, and act more safely without adding unnecessary friction to their role.

For assurance purposes, this means Cyber Rebels operates as an education-led provider rather than a generic content vendor. Training is delivered live by qualified educators with relevant cybersecurity experience, and engagements are designed to fit around client processes, safeguarding requirements, and operational realities.

2. Services and delivery overview

Cyber Rebels delivers instructor-led cybersecurity and digital safety training across business, education, youth, and community settings. Sessions may be delivered remotely or on site, depending on client need, and are shaped around the audience's responsibilities, existing controls, and risk environment.

Programmes are designed to be practical, age-appropriate, and relevant to real situations rather than abstract awareness messaging. Delivery can include demonstrations, facilitated discussion, scenario-based exercises, reflective activities, and applied guidance aligned to the organisation's context. Where required, Cyber Rebels works with client stakeholders in advance to confirm delivery boundaries, escalation routes, safeguarding arrangements, and any data handling considerations connected to the session.

Cyber Rebels also aligns delivery with relevant organisational policies where appropriate, including safeguarding procedures, acceptable use expectations, incident escalation routes, and internal security requirements. This helps ensure training supports existing governance rather than operating separately from it.

3. Governance, policies, and compliance

Cyber Rebels maintains a suite of governance and compliance documents to support lawful, safe, and transparent delivery. These documents are reviewed and updated to reflect changes in legislation, guidance, technology, and operational practice.

The policy set is written with reference to the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, Cyber Essentials principles, National Cyber Security Centre guidance, and relevant sector-specific requirements across education, business, charity, and public-facing environments. As safeguarding-led work forms part of the offer, the organisation also takes account of current safeguarding expectations where these affect delivery design or operational controls.

The current policy library is available through the Cyber Rebels policy hub:

https://cyber-rebels.co.uk/our-policies-and-terms

The available documentation includes, but is not limited to, the following:

- Privacy Policy
- Cookies and Tracking Policy

- Information Security Policy
- Data Retention Schedule
- Youth DPIA and Safeguarding Policy
- Cyber Hygiene Commitment
- Complaints Policy
- Health and Safety Policy
- Training Services Terms and Conditions and website terms

4. Data protection and information security

Data protection is treated as an operational discipline rather than a paperwork exercise. Cyber Rebels follows a minimum necessary approach to data collection and retention, limiting the personal information it receives, stores, and processes to what is reasonably required for delivery, administration, safeguarding, or lawful business operations.

Technical and organisational measures are used to protect information appropriately. These include encrypted local storage, access controls, multi-factor authentication across systems, device hardening, secure configuration, and the use of digitally certified communications where authenticity and message integrity matter. The organisation also maintains a Data Retention Schedule and uses a defined deletion approach for temporary materials generated during delivery activities or demonstrations.

Cyber Rebels states that it does not sell personal data, disclose it to third parties without an appropriate lawful basis, or retain it beyond what is necessary for the stated purpose. For youth and education delivery, the organisation maintains a dedicated DPIA. It also maintains a Legitimate Interests Assessment, together with a public summary, where that lawful basis is relied upon.

5. Safeguarding and learner safety

Cyber Rebels works with schools, trusts, youth groups, clubs, and community organisations, so safeguarding is treated as a core delivery control. Youth-focused activity is shaped around current statutory and operational safeguarding expectations, including Keeping Children Safe in Education, online safety considerations such as the Ofsted 4Cs, the organisation's own youth-focused DPIA arrangements, and the safeguarding procedures of the partner setting. The aim is not only to deliver suitable content, but to ensure the delivery model itself remains safe, proportionate, and easy for the partner organisation to oversee.

The organisation's stated controls for youth delivery include limiting data collection, avoiding unnecessary personal disclosures from participants, keeping a responsible adult present throughout delivery, operating a no-recording rule for youth participants, using age-appropriate language and examples, and routing any concern or escalation through the client organisation's designated safeguarding process. Temporary youth-related data created for delivery purposes is deleted shortly after use.

Cyber Rebels has stated that all personnel involved in youth delivery hold Enhanced DBS certificates and that delivery is conducted in line with the safeguarding policies and local procedures of the organisation being supported. This matters from an assurance perspective because it makes clear that Cyber Rebels is not attempting to replace the client's safeguarding framework. It works within it.

6. Professional standards and training quality

Training is delivered as a live educational service rather than a passive content product. Sessions are designed to be clear, structured, relevant to the audience, and manageable in real settings, whether that means a primary school class, a staff team, a youth group, a remote workforce, or a leadership workshop.

Cyber Rebels states that delivery is carried out by qualified cybersecurity educators holding recognised teaching and assessment credentials, including the Level 3 Award in Education and Training and the Level 3 Award in Assessing Competence in the Work Environment. In addition, the organisation references professional recognition with bodies including BCS, CIISec, and ISACA. This combination of educational and subject-matter capability supports delivery that is both technically credible and pedagogically appropriate.

Programmes are described as CPD-accredited and are built around practical relevance rather than fear-based messaging. Delivery can include demonstrations, simulations, reflective discussion, and scenario-based learning. The intention is to strengthen understanding and judgement in ways that people can apply in their real role, rather than relying on short-term awareness alone.

7. Training methodology and behavioural framework

Cyber Rebels uses a defined behavioural competency framework known as the Five-Domain Model. This model is used to design, deliver, and quality-control training across sectors and audiences, helping ensure a consistent standard of delivery while still allowing the session to be adapted to client context.

The model covers contextual risk recognition, verification and control discipline, secure operational behaviour, incident judgement and escalation, and professional cyber judgement. In practice, this means training is not structured solely around topics or threat lists. It is structured around the decisions participants need to make in ordinary work, the pressures that make those decisions difficult, and the behaviours that help reduce avoidable risk.

From a due diligence perspective, the value of this framework is consistency. It provides Cyber Rebels with a repeatable way to plan sessions, map activities, and evaluate behavioural outcomes without defaulting to generic awareness delivery. It also supports clearer alignment between client context, training objectives, and the practical judgements people are expected to make during normal work.

8. Security practices and technical controls

Cyber Rebels states that its own internal security practices reflect the standards it expects in delivery. The organisation describes a secure-by-default, simple-by-design approach, intended to reduce avoidable exposure by limiting data, limiting access, and avoiding unnecessary complexity.

Operational controls identified within the source material include encrypted data storage, multi-factor authentication on all systems, device hardening, secure configuration, secure networks and VPN use where required, regular security and policy review activity, and restrictions on the use of USB or removable media in youth settings. These measures support the wider data protection and operational assurance position presented in this pack.

9. Insurance, registrations, and organisational assurance

Cyber Rebels has confirmed that it maintains Public Liability cover of £2,000,000, Professional Indemnity cover of £1,000,000, and Cyber Insurance cover of £1,000,000. Insurance certificates can be supplied on request as part of procurement or onboarding checks.

The organisation has also provided the following registration details for assurance purposes: ICO registration number ZB892477 and UKPRN 10098239. Additional supporting evidence, including policy extracts, certificates, and qualification documents, is available on request where needed for formal supplier checks.

10. Ethical practice and sustainability

Cyber Rebels positions ethical practice as part of service quality rather than as a separate statement of intent. Its source material emphasises accurate communication, age-appropriate and inclusive delivery, respect for learner wellbeing, and avoidance of exaggerated or fear-based messaging. It also states that trainers work within clear standards for professional conduct, impartiality, safeguarding responsibility, confidentiality, and responsible use of technology.

The organisation also states that it operates transparently with partners, discloses conflicts where relevant, and maintains clear boundaries around data privacy and confidentiality. In operational terms, this supports a lower-friction working relationship for client organisations because expectations around conduct, information handling, and delivery boundaries are made explicit rather than assumed.

On sustainability, Cyber Rebels notes that it operates primarily through digital delivery where appropriate in order to reduce travel emissions and waste, and that it holds Green Small Business certification. Verification documents can be provided on request.

11. Working arrangements with client organisations

Cyber Rebels describes its delivery model as collaborative and pre-planned rather than transactional. Before delivery begins, the organisation works with the client to understand the audience, operating environment, safeguarding requirements, and any relevant organisational

constraints. This includes confirming whether personal data is required, agreeing age group or learner profile where relevant, and ensuring the session design fits the setting rather than expecting the setting to fit a fixed product.

This approach reduces friction for the client because the important questions are addressed before delivery rather than during it. For procurement, assurance, and operational leads, that means Cyber Rebels is positioning itself as a provider that can slot into existing governance arrangements and delivery expectations with a clear understanding of boundaries and responsibilities.

12. Documents available on request

The following supporting documents can be provided to partner organisations where required for onboarding, due diligence, safeguarding checks, or procurement review:

- Enhanced DBS certificates
- Professional qualifications and teaching credentials
- CPD accreditation certificate
- Insurance certificates
- ICO registration details
- Data protection documentation, including LIA, DPIA, and retention schedule materials
- Safeguarding and online safety policies
- Accessibility information and reasonable adjustment details
- UKPRN registration details

13. Contact and escalation details

General enquiries	hello@cyber-rebels.co.uk
Safeguarding lead	Andy Longhurst
Data protection contact	andy.longhurst@cyber-rebels.co.uk

14. Statement of assurance

Cyber Rebels confirms that the policies and controls referenced in this assurance pack are maintained and reviewed as part of normal operations. The organisation states that its services are delivered in line with applicable UK data protection law, relevant safeguarding expectations, and the operational security measures described in this document.

In practical terms, the assurance position presented here is straightforward: Cyber Rebels aims to deliver training in a way that is safe, compliant, professionally managed, and easy for partner organisations to evaluate. It is intended to give procurement, compliance, safeguarding, and assurance reviewers a clear summary of the organisation's operating approach without requiring them to extract that information from broader marketing or website content.