



PARTNER & SUPPLIER ASSURANCE PACK

Version 4.2 - July 2026



WEBSITE:

cyberrebels.co.uk

PHONE:

07473 256429

EMAIL:

hello@cyberrebels.co.uk

Supplier Assurance Pack

This supplier assurance pack supports due diligence, procurement review and late-stage assurance checks.

It has been prepared to help organisations understand how Cyber Rebels Ltd operates, how training is delivered, and what governance, safeguarding, data protection, cyber resilience and compliance arrangements are in place.

What this pack helps you verify

Governance, safeguarding, data protection, cyber resilience, training quality, insurance, professional standards and the evidence available to support procurement or assurance review.

Contents

1-3	Purpose, organisation and delivery
4-7	Governance, data protection, safeguarding and professional standards
8-9	Training methodology and evidence
10-11	Security, cyber resilience and supplier assurance
12-17	Insurance, ethics, working arrangements, evidence and assurance statement

1. Purpose of this assurance pack

This document provides a clear overview of Cyber Rebels Ltd, the services we deliver, the standards we work to, and the supporting documentation available for supplier validation.

It is intended for procurement, compliance, safeguarding, data protection and assurance-led review processes. It may be used by schools, trusts, businesses, community organisations, regulated sectors and partner organisations that need confidence that Cyber Rebels can deliver training safely, professionally and responsibly.

Cyber Rebels approaches cybersecurity as a practical human issue shaped by how people work, communicate and make decisions in real environments. That view influences how we design training, handle information, manage safeguarding responsibilities and work with organisations before, during and after delivery.

2. About Cyber Rebels Ltd

Cyber Rebels Ltd is a UK training provider delivering live, instructor-led cybersecurity and digital safety training for schools, businesses, youth organisations, community groups, SMEs and regulated sectors.

Our sessions are practical, clear and relevant to the environments people actually work and learn in. We operate as educators first, so delivery is shaped around clarity, professionalism, safeguarding, learner support

and practical understanding rather than fear-based messaging or generic awareness content.

Our work helps people make safer, more confident decisions in digital environments without making cybersecurity feel abstract, technical or inaccessible.

Cyber Rebels is a CPD Approved Provider, and eligible programmes can support CPD requirements. Sessions can be adapted to organisational context, audience type, safeguarding requirements and operational risk profile. We work with partner organisations to ensure delivery aligns with their internal policies, conduct expectations, safeguarding arrangements and information security requirements.

3. Services and delivery overview

Cyber Rebels provides live, interactive cybersecurity and digital safety training across a range of settings.

Delivery may include business cybersecurity training, education-focused sessions, youth digital safety sessions, awareness workshops and behaviour-led cybersecurity training tailored to organisational context.

Sessions are built around realistic situations, practical decision-making and clear explanation. Depending on the audience, training may include guided discussion, structured demonstrations, reflective activities, scenario-based learning and age-appropriate interactive exercises.

We work with children, young people, adults, remote teams, SMEs, frontline staff and regulated sectors. Where delivery takes place in education or youth settings, the content and format are adapted to suit the age group, learning environment, safeguarding requirements and operational expectations of the partner organisation.

4. Governance, policies and compliance

Cyber Rebels maintains governance, policy and compliance documentation to support safe, lawful and transparent delivery.

These policies are reviewed regularly and updated where needed in line with changes in legislation, technology, operational practice, safeguarding guidance and sector expectations.

Our documentation is written with reference to UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, Cyber Essentials principles, NCSC guidance, and relevant safeguarding and sector-specific requirements.

Cyber Rebels Ltd was among the first 100 organisations listed as signatories to the UK Government Cyber Resilience Pledge. As part of that commitment, Cyber Rebels has registered for the NCSC Early Warning service, added its domain and IPv4 assets through MyNCSC, and completed approved registration for the Cyber Essentials Supplier Check Tool.

Early signatory

Cyber Rebels Ltd was among the first 100 organisations listed as signatories to the UK Government Cyber Resilience Pledge.

Current policies are available at: cyberrebels.co.uk/our-policies-and-terms

Available policies include:

- 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

Terms and Conditions

Business Continuity and Disaster Recovery Plan

5. Data protection and information security

Data protection is built into how Cyber Rebels operates.

We follow a data minimisation approach, collecting only what is necessary, limiting what is retained, and applying appropriate technical and organisational controls to protect the information we handle.

Our data protection arrangements include a Legitimate Interest Assessment and public summary where relevant, a full Data Protection Impact Assessment for youth and education services, encryption for locally stored files, access controls, secure communications and a documented data retention schedule.

We do not sell personal data, share it without a lawful basis, or retain it for longer than necessary.

Where temporary data is used during delivery, such as for activities or demonstrations, it is managed carefully and deleted where appropriate shortly after use.

6. Safeguarding children and young people

Cyber Rebels works with schools, trusts, youth groups, clubs and community organisations. Safeguarding is treated as a core operational responsibility.

Our youth-focused work is shaped by Keeping Children Safe in Education, the Ofsted 4Cs framework, UK data protection requirements, youth-specific DPIAs and the safeguarding expectations of the organisation we are supporting.

Our delivery model is designed to reduce unnecessary safeguarding risk. We do not require sensitive or unnecessary personal disclosures from young people. A responsible adult from the partner organisation is expected to be present throughout delivery. Content is age-appropriate, recording is not permitted for youth participants, and any safeguarding concerns are escalated through the organisation's own safeguarding lead and procedures.

Cyber Rebels personnel working in relevant settings must hold an appropriate Enhanced DBS certificate. Where delivery support is used, this requirement is confirmed before the individual is assigned to the work.

We also follow the safeguarding policies, procedures and practical guidance of each partner organisation when operating in their environment.

7. Professional standards and training quality

Cyber Rebels training is designed to be safe, relevant and professionally structured.

Sessions are fully instructor-led and adapted to the needs of the audience, whether that audience is made up of pupils, staff teams, youth groups, remote workers, operational teams or senior leaders.

Training is delivered by qualified cybersecurity educators who hold 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.

These qualifications support effective learning design, inclusive delivery, learner engagement and safe session management across youth and adult environments.

Alongside teaching qualifications, our trainers bring practical cybersecurity knowledge and professional recognition, including membership or affiliation with bodies such as BCS, CII Sec and ISACA.

This combination of educational capability and industry understanding helps ensure sessions are structured, appropriate and grounded in real-world relevance.

8. Training methodology and behavioural framework

Cyber Rebels training is designed and quality-controlled using a defined behavioural competency structure known as the Five-Domain Model.

This model provides a consistent foundation for planning, delivery and review across different sectors, audiences and formats.

The Five-Domain Model

- Contextual Risk Recognition
- Verification and Control Discipline
- Secure Operational Behaviour
- Incident Judgement and Escalation
- Professional Cyber Judgement

These domains are used to shape session design and keep training focused on how people recognise, interpret and respond to situations in practice.

This matters because cybersecurity training is most useful when it reflects the conditions people actually work in. A person may understand general guidance, but still need support applying it when a request looks familiar, a task is time-sensitive, or the right response is not immediately obvious.

The Five-Domain Model helps Cyber Rebels design training around those practical moments. Activities are mapped against the domains during planning and delivery so training remains relevant to the client environment while following a structured and repeatable quality framework.

9. How training quality is evidenced

Cyber Rebels does not measure training quality only by attendance or completion.

Those records may support delivery assurance, but they do not show whether training has helped people make better decisions in practice.

Our quality approach looks for evidence of changed recognition, clearer language, better verification habits, earlier escalation and more confident discussion of uncertainty.

That may include participants recognising where a normal-looking request still needs checking, identifying why a shortcut felt reasonable, naming the point where a decision should be paused, or explaining when something should be escalated before it becomes clearly serious.

This kind of evidence may appear through scenario discussion, reflective activities, participant questions, decision mapping and the language people use when working through realistic situations.

The aim is not simply that people know more. It is that they leave better able to recognise, check, question and escalate in the kinds of situations they are likely to face during normal work.

For supplier assurance, training quality is considered through both delivery standards and practical behavioural relevance: whether the session was managed professionally, whether the content was appropriate for the audience, and whether the learning helped people make sense of real decisions they may need to handle afterwards.

10. Security practices and technical measures

Cyber Rebels applies practical security measures across its operations and uses the same standards of sensible cyber hygiene that it promotes in training.

Operational measures include encrypted data storage, multi-factor authentication on systems, secure configuration, device hardening, appropriate network security and regular review of security and policy controls.

Cyber Rebels is registered for the NCSC Early Warning service. Relevant domain and IPv4 assets have been added through MyNCSC to support early notification of potential cyber threats affecting the business.

Where relevant, we avoid the use of removable media in youth settings, use secure communications, and apply a simple-by-design approach that reduces unnecessary access, unnecessary retention and unnecessary risk.

11. Cyber resilience and supplier assurance

Cyber Rebels Ltd was among the first 100 organisations listed as signatories to the UK Government Cyber Resilience Pledge.

The pledge reinforces our commitment to treat cyber resilience as a leadership responsibility, use national cyber warning services and review the security arrangements of the suppliers and digital platforms our work depends on.

Completed pledge actions

- Submitted its signed pledge declaration to DSIT and received confirmation of participation
- Registered for the NCSC Early Warning service
- Added its domain and IPv4 assets through MyNCSC
- Registered for the Cyber Essentials Supplier Check Tool, with the registration approved

Cyber Rebels is continuing its proportionate review of suppliers and digital platforms in line with the pledge commitments. Supplier assurance decisions are recorded according to the service involved, the information or access available to the supplier, and the level of operational dependency.

12. Insurance

Cyber Rebels maintains appropriate business insurance cover to support delivery and supplier assurance requirements.

Public Liability insurance	£2,000,000
Professional Indemnity insurance	£1,000,000
Cyber Insurance	£1,000,000

Insurance certificates can be provided on request.

13. Sustainability and ethical practice

Cyber Rebels is committed to operating responsibly, transparently and in a way that supports trust, fairness and long-term accountability.

We do not rely on fear-based messaging, exaggerated claims or manipulative delivery practices. Our training supports people through clear explanation, practical relevance and respectful communication.

We work openly with partner organisations, disclose relevant information clearly, and maintain appropriate professional boundaries around data use, confidentiality, safeguarding and conduct.

We do not accept inducements that would compromise integrity, and we expect professional standards to be maintained across delivery, communication and operational practice.

We also seek to reduce unnecessary environmental impact through digital-first delivery where appropriate. Cyber Rebels holds Green Small Business certification, and supporting evidence can be provided on request.

14. Working with your organisation

Cyber Rebels works collaboratively with each organisation before delivery begins.

This allows us to understand the environment, the intended audience, relevant safeguarding or leadership contacts, any data requirements, and the practical considerations that need to be reflected in the session.

Where relevant, we confirm age group, safeguarding expectations, delivery format, session boundaries and any reasonable adjustments required to support safe and effective participation.

This helps ensure the session fits naturally within your existing processes rather than creating unnecessary friction.

Our approach is straightforward and professional. We adapt to the organisation we are supporting and aim to deliver in a way that is safe, efficient and aligned with the standards already in place.

15. Documents available on request

- Enhanced DBS certificates
- Professional qualifications
- CPD Approved Provider evidence
- Insurance certificates
- ICO registration details
- Data protection documentation, including LIA, DPIA and retention schedules
- Safeguarding and online safety policies
- Accessibility information and reasonable adjustments details
- UKPRN registration details
- Green Small Business certification evidence
- Cyber Resilience Pledge declaration and DSIT confirmation
- NCSC Early Warning registration evidence
- Cyber Essentials Supplier Check Tool registration confirmation

16. Operational and contact details

General enquiries	hello@cyberrebels.co.uk
Safeguarding lead	Andy Longhurst
Data protection contact	hello@cyberrebels.co.uk
ICO Registration	ZB892477
UKPRN	10098239

17. Statement of assurance

Cyber Rebels confirms that the policies and controls referenced in this document are maintained and reviewed regularly.

We operate in alignment with UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, and relevant safeguarding and security frameworks applicable to the environments in which we work.

Where delivery involves children and young people, safeguarding requirements are treated as an operational priority. Sessions are planned and delivered with appropriate supervision, age suitability, data protection and escalation arrangements in place.

Where delivery involves staff teams, businesses or regulated environments, training is shaped around the organisation's context, audience and operational expectations so that delivery remains practical, proportionate and professionally managed.

Statement of assurance

Our aim is to give partner organisations clear assurance that Cyber Rebels can support delivery safely, credibly and without creating unnecessary procurement or compliance friction.