

PRIVACY POLICY

Decrypthut Limited
Effective: September 2026

1. Who we are

Decrypthut Limited (“Decrypthut”, “we”, “us” or “our”) provides technology education, training, workshops, courses, roadshows, mentoring, workforce development and related learning and innovation activities.

Decrypthut Limited is a company registered in England and Wales under company number **13085156**.

Registered office:

71–75 Shelton Street
London
WC2H 9JQ
United Kingdom

For the purposes of UK data protection law, Decrypthut Limited is the controller of personal information covered by this Privacy Policy unless another organisation is expressly identified as the controller.

Questions about privacy or requests concerning your personal information can be sent to:

info@decrypthut.com

2. Scope

This Privacy Policy explains how we collect and use personal information when you:

- visit our website;
- contact us;
- register for or participate in a Decrypthut programme;
- attend a workshop, course, roadshow or event;
- receive mentoring or other learning support;
- earn a Decrypthut digital badge;
- work with us through a school, council, employer, community organisation or other partner;
- apply to work with or for Decrypthut;
- appear in authorised photographs, video or other media; or
- otherwise interact with Decrypthut.

Where a school, local authority, employer or other organisation provides information to us or commissions a programme, that organisation may also be a controller of your information. Its own privacy notice may therefore also apply.

3. Information we collect

Depending on your relationship with us, we may collect:

Identity and contact information

This may include:

- name;
- age or date of birth where required;

- email address;
- telephone number;
- parent or guardian details;
- organisation, school or employer;
- job title; and
- emergency contact information where appropriate.

Programme and learning information

This may include:

- programme registration;
- attendance;
- course participation;
- projects and work produced;
- assessment or challenge results;
- skills developed;
- progress;
- learner feedback;
- survey responses;
- digital badges and achievements;
- mentoring records where applicable; and
- information necessary to provide or evaluate a programme.

Learning support information

Where necessary, we may receive information concerning:

- disability;
- health;
- SEN;
- neurodivergence;
- accessibility requirements;
- reasonable adjustments;
- communication requirements; or
- other information needed to support safe and inclusive participation.

Some of this information constitutes special-category personal data and receives additional protection under data protection law.

Safeguarding information

Where a safeguarding or welfare concern arises, we may process information concerning a child or adult, the concern raised, actions taken, relevant communications and information required for safeguarding purposes.

Photographs, video and audio

Where appropriate, Decrypthut may take or receive photographs, video or audio from programmes and events.

Our approach to photographs and recordings is explained in section 10.

Business information

When working with schools, councils, employers, suppliers, universities, community organisations and corporate partners, we may process professional contact information and correspondence.

Website and technical information

When you use our website, certain technical information may be collected, including:

- IP address;
- browser and device information;
- pages visited;
- website interactions;
- approximate technical location information;
- cookie preferences; and
- diagnostic and security information.

4. How we collect information

We may receive information:

- directly from you;
- from your parent or guardian;
- from a school or educational institution;
- from a local authority;
- from your employer;
- from a commissioning or community organisation;
- from facilitators or programme delivery partners;
- through forms, surveys or programme registration;
- through our website;
- through correspondence with us; and
- where appropriate, from safeguarding or statutory bodies.

5. How we use personal information

We may use personal information to:

- respond to enquiries;
- administer programme registrations;
- deliver workshops, courses, mentoring, roadshows and other services;
- communicate with learners, parents, guardians and organisations;
- support individual learning needs;
- make reasonable adjustments;
- maintain attendance and participation records;
- recognise learner achievements;
- issue and administer digital badges;
- provide programme feedback and learner support;
- evaluate programme quality and outcomes;
- improve our programmes and services;
- administer partnerships and contracts;
- manage safeguarding and welfare concerns;
- maintain the safety and security of our website and systems;
- prevent fraud or misuse;
- manage complaints;
- establish, exercise or defend legal claims;
- comply with legal and regulatory requirements; and
- promote Decrypthut where we have an appropriate lawful basis to do so.

We do not sell personal information.

6. Our lawful bases

We only use personal information where we have a lawful basis.

Depending on the circumstances, this may be:

Contract

Where processing is necessary to provide a service, administer a booking or fulfil an agreement with you.

Legitimate interests

Where processing is reasonably necessary for the operation, administration, security, development or improvement of Decrypthut and those interests are not overridden by your rights.

Consent

Where you have freely chosen to give permission for a particular use, including certain marketing activities and photography or promotional media.

Where we rely on consent, you may withdraw it.

Legal obligation

Where we must process information to comply with a legal requirement.

Vital interests

In exceptional circumstances where processing is necessary to protect someone's life.

7. Special-category information

Information about health, disability and certain other sensitive matters may constitute special-category personal data.

Where we process special-category information, we identify both an appropriate lawful basis and an additional condition permitted by UK data protection law.

Depending on the circumstances, this may include explicit consent, substantial public interest grounds provided for by law, safeguarding-related conditions, or other applicable conditions.

We seek to collect only the information genuinely necessary for the relevant purpose and restrict access appropriately.

8. Children and young people

Children and young people are an important part of Decrypthut's work.

We take particular care when collecting and using their personal information.

Information should be presented in a way appropriate to the age and understanding of the child where appropriate.

Depending on the programme, information may be provided by a parent, guardian, school, council or commissioning organisation.

We aim to collect only information reasonably necessary to:

- deliver the programme;

- keep learners safe;
- provide appropriate support;
- recognise achievement;
- communicate appropriately; and
- meet our legal or contractual responsibilities.

A child's information will not be used for an unrelated purpose merely because we already hold it.

9. Digital badges and Sertifier

Decrypthut uses Sertifier, a third-party digital credential platform, to issue, manage, host and verify Decrypthut digital badges and certificates.

Where you earn a Decrypthut digital credential, we may provide Sertifier with the information reasonably necessary to create and administer that credential. This may include:

- your name;
- email address;
- programme or activity completed;
- credential awarded;
- skills or learning outcomes recognised;
- achievement criteria;
- issue date;
- expiry date, where applicable;
- credential identifier; and
- information required to verify the credential.

Sertifier may provide learners with access to a digital credential page, wallet or verification function and may enable learners to download or share their credential.

Learners are not required to publish or share their credential publicly simply because it has been awarded.

Decrypthut determines the credential awarded, the criteria associated with it and the achievement it represents. Sertifier provides the technology used to issue and verify the credential.

We only share information with Sertifier that is reasonably necessary for the administration and verification of Decrypthut credentials.

Sertifier processes personal information in accordance with its own privacy arrangements and applicable contractual and data protection requirements.

Personal information associated with Decrypthut digital badges is otherwise handled in accordance with this Privacy Policy.

10. Photography, video and use of images

We use real programme imagery because it helps demonstrate Decrypthut's work and impact. We also recognise that learners must have meaningful control over how identifiable images of them are used.

Photographs, video or audio may be taken during Decrypthut programmes, workshops or events for purposes including:

- documenting programme activity;
- impact reporting;
- programme evaluation;
- Decrypthut's website;
- presentations and proposals;

- social media;
- promotional and informational materials; and
- communications concerning Decryphtut's work.

Consent

Where consent is the appropriate basis for identifiable promotional photography or recording, we will obtain appropriate permission.

For children, this will normally involve permission from a parent or guardian where appropriate, while also respecting the wishes of the child.

A learner who does not wish to be photographed or recorded will not be excluded from the educational programme merely for refusing promotional photography consent.

Where practical, photographers and programme staff will be informed of individuals who should not appear in identifiable promotional images.

Withdrawing permission and requesting removal

Consent to the future use of an identifiable photograph or recording may be withdrawn at any time by contacting:

info@decryphtut.com

Please provide enough information for us to identify the relevant image or recording.

Where consent is withdrawn, Decryphtut will stop new uses of the relevant identifiable image and, where reasonably practicable, remove it from websites, social-media accounts and other digital channels under Decryphtut's control.

Withdrawal does not make previous lawful use of an image unlawful.

It may not always be possible to retrieve:

- printed materials already distributed;
- material already lawfully published or supplied to third parties;
- copies independently saved, reposted or shared by other people; or
- material that Decryphtut is legally required to retain.

However, we will take reasonable steps within our control in response to a valid removal request.

We will not normally publish a child's full name alongside an identifiable image unless there is a clear reason and appropriate permission.

11. Safeguarding

Safeguarding information may need to be used or disclosed where necessary to protect a child or another person.

Depending on the circumstances, information may be shared with:

- a school's Designated Safeguarding Lead;
- a commissioning organisation;
- a local authority;
- children's social care;
- the police;

- emergency services; or
- another appropriate safeguarding body.

Where there is a safeguarding risk, we may share relevant information without consent where the law permits or requires this.

Our safeguarding arrangements are set out in our Safeguarding and Child Protection Policy.

12. Who we share information with

Where necessary and lawful, information may be shared with:

- schools;
- local authorities;
- commissioning organisations;
- employers;
- parents or guardians;
- programme delivery partners;
- authorised facilitators, tutors and contractors;
- technology providers;
- badge or credential providers;
- professional advisers;
- insurers;
- safeguarding bodies;
- regulators;
- law-enforcement agencies; and
- courts or other authorities where required.

We require service providers handling information on our behalf to protect it appropriately.

13. International transfers

Some technology providers may process information outside the United Kingdom.

Where personal information is transferred internationally, we take appropriate steps required by UK data protection law, which may include reliance on UK adequacy regulations or approved contractual safeguards.

14. Marketing

We may send information about Decrypthut programmes, opportunities or services where permitted by law.

Where consent is required, we will obtain it.

You may opt out of direct marketing at any time by using an unsubscribe facility where provided or contacting:

info@decrypthut.com

We may retain limited information necessary to record and respect an opt-out request.

15. Retention

We keep personal information only for as long as reasonably necessary for the purpose for which it was collected, including applicable legal, contractual, safeguarding, insurance and dispute-resolution requirements.

Safeguarding records may need to be retained for longer periods because concerns can remain relevant after programme participation ends.

When information is no longer required, it will be securely deleted, destroyed or anonymised as appropriate.

16. Security

We use appropriate technical and organisational measures designed to protect personal information from:

- unauthorised access;
- loss;
- misuse;
- disclosure;
- alteration; and
- destruction.

Access to personal and safeguarding information is restricted according to role and need.

17. Your rights

Depending on the circumstances, you may have the right to:

- access personal information we hold about you;
- correct inaccurate or incomplete information;
- request deletion;
- request restriction of processing;
- object to certain processing;
- receive certain information in a portable format;
- withdraw consent where consent is relied upon; and
- complain about how your information has been handled.

These rights are not absolute and legal exceptions may apply.

To exercise a right, contact:

info@decrypthut.com

We may need to verify your identity before responding.

18. Complaints

If you have concerns about how Decrypthut uses your personal information, please contact us first at:

info@decrypthut.com

You also have the right to complain to the UK Information Commissioner's Office.

19. Cookies

Our website uses cookies and similar technologies as described in our Cookie Policy.

20. Changes to this policy

We may update this Privacy Policy to reflect changes to our services, technology, business or legal requirements.

The current version will be published on our website.

Decrypthut Limited

Company number: **13085156**

71–75 Shelton Street, London, WC2H 9JQ

info@decrypthut.com

SAFEGUARDING AND CHILD PROTECTION POLICY

Decrypthut Limited

Effective: September 2026

Review date: September 2027

1. Our commitment

Decrypthut is committed to safeguarding and promoting the welfare of every child and young person who participates in our programmes.

The welfare and safety of the child are paramount.

No member of staff, facilitator, contractor, volunteer or other person acting on behalf of Decrypthut may inflict physical, sexual, emotional or psychological harm on a child.

Every person working on behalf of Decrypthut shares responsibility for creating safe learning environments, recognising concerns and reporting them appropriately.

2. Scope

This policy applies to:

- directors;
- employees;
- facilitators;
- tutors;
- mentors;
- contractors;
- consultants;
- volunteers;
- university students or graduates engaged in delivery;
- creative and technical specialists; and
- anyone otherwise acting on behalf of Decrypthut.

It applies to Decrypthut activities delivered:

- in person;
- online;
- in schools;
- in community settings;
- at partner venues;
- through workshops and courses;
- through roadshows;

- through mentoring;
- through events; and
- through other Decrypthut programmes.

For this policy, a child is anyone under 18.

3. Designated Safeguarding Lead

Decrypthut's Designated Safeguarding Lead ("DSL") is:

Michaela Carew
Founder & CEO, Decrypthut Limited
info@decrypthut.com

The DSL is responsible for overseeing safeguarding practice, receiving concerns, maintaining appropriate records, supporting staff and determining when concerns need to be referred to another organisation or statutory authority.

Where Decrypthut is delivering within a school, council facility or partner setting, the host organisation's safeguarding procedures and DSL arrangements must also be identified before delivery.

If there is an immediate risk of serious harm, staff must contact **999** rather than waiting for the DSL.

4. Principles

Decrypthut will:

- put children's welfare first;
- listen to children and take concerns seriously;
- treat children with dignity and respect;
- provide inclusive learning environments;
- maintain appropriate professional boundaries;
- respond promptly to safeguarding concerns;
- minimise opportunities for abuse or inappropriate conduct;
- recognise online and technology-related safeguarding risks;
- consider additional vulnerabilities associated with SEN, disability or communication differences;
- work appropriately with parents, schools, councils and safeguarding agencies; and
- maintain appropriate safeguarding records.

5. Safer recruitment and suitability

People working with children on behalf of Decrypthut must be suitable for their role.

Depending on the role and its eligibility under applicable law, Decrypthut's checks may include:

- identity verification;
- employment or activity history;
- references;
- interview or suitability assessment;
- right-to-work checks;
- relevant qualification checks;
- appropriate Disclosure and Barring Service checks, including barred-list information where the role is legally eligible;
- safeguarding induction; and
- ongoing supervision.

A DBS check will only be requested at the level legally available and appropriate for the role.

No person should undertake regulated activity with children unless applicable safeguarding and suitability requirements have been completed.

6. Code of conduct

Adults working with children must:

- behave professionally;
- treat learners fairly and respectfully;
- maintain appropriate physical and emotional boundaries;
- use appropriate language;
- use authorised communication channels;
- avoid unnecessary private communication with children;
- avoid inappropriate one-to-one situations;
- never pursue or encourage a sexual or romantic relationship with a child;
- never engage in bullying, harassment, discrimination or intimidation;
- never exchange inappropriate images or messages;
- never use personal social-media relationships as a means of communicating privately with children;
- never consume alcohol or illegal drugs while responsible for learners; and
- report safeguarding concerns.

Staff must not promise a child complete confidentiality where safeguarding information is disclosed.

7. Recognising safeguarding concerns

Concerns may relate to:

- physical abuse;
- sexual abuse;
- emotional abuse;
- neglect;
- domestic abuse;
- bullying;
- cyberbullying;
- grooming;
- sexual harassment;
- sexual violence;
- child-on-child abuse;
- exploitation;
- online abuse;
- harmful or inappropriate online content;
- discrimination;
- self-harm or serious welfare concerns;
- radicalisation;
- inappropriate adult conduct; or
- any other situation in which a child may be at risk of harm.

Staff are not responsible for investigating suspected abuse.

Their responsibility is to **recognise, respond, record and report**.

8. Responding to a disclosure

If a child discloses something that may indicate harm:

1. listen calmly;
2. take the child seriously;

3. do not express disbelief;
4. do not interrogate the child;
5. ask only questions necessary to clarify what is being said;
6. do not promise secrecy;
7. explain that the information needs to be shared with someone who can help;
8. make a factual written record as soon as possible; and
9. report the concern immediately.

Records should distinguish clearly between what the child said, what was observed and any professional judgement.

9. Reporting concerns

Concerns must be reported promptly to the Decrypthut DSL.

Where delivery takes place within a school or other partner setting, the host organisation's DSL or safeguarding lead must also be informed where its procedures require this.

Depending on the concern, information may need to be referred to:

- children's social care;
- the relevant local authority;
- the Local Authority Designated Officer where appropriate;
- the police;
- emergency services;
- the Disclosure and Barring Service; or
- another relevant safeguarding authority.

If a child appears to be in immediate danger, call **999**.

A concern must not be ignored simply because the person reporting it does not have complete evidence.

10. Allegations or concerns about adults

Any allegation that a person working for or with Decrypthut has:

- harmed a child;
- possibly committed an offence involving a child;
- behaved in a way indicating they may pose a risk to children; or
- behaved in a way that raises concern about their suitability to work with children

must be reported immediately to the DSL.

Where the concern relates to the DSL, it should be reported to another Decrypthut director or, where appropriate, directly to the relevant local authority safeguarding service.

Decrypthut will not conduct an internal investigation in a way that compromises a police, local-authority or other statutory investigation.

Appropriate referral obligations will be followed.

11. Child-on-child abuse and bullying

Abuse between children will not be dismissed as “banter”, normal behaviour or part of growing up.

Concerns involving bullying, sexual harassment, sexual violence, discriminatory behaviour, coercion, online abuse or other harmful behaviour between children will be taken seriously and addressed through safeguarding procedures.

Both the child who may have experienced harm and other children involved should receive appropriate consideration and support.

12. Online safety

Because Decrypthut teaches technology, online safety forms a core part of our safeguarding approach.

Relevant risks include:

- inappropriate content;
- cyberbullying;
- grooming;
- sexual exploitation;
- sharing personal information;
- harmful communications;
- impersonation;
- scams and fraud;
- misuse of AI;
- unsafe online communities;
- inappropriate image sharing; and
- unauthorised contact between adults and children.

Adults should use approved platforms and professional accounts when communicating with learners.

Personal social-media accounts must not be used to establish private relationships with children participating in Decrypthut programmes.

Online sessions must be delivered using appropriate safeguarding arrangements.

13. AI and emerging technologies

Where AI or other emerging technologies are used during learning, facilitators should consider:

- age appropriateness;
- privacy;
- personal information entered into systems;
- harmful or inaccurate content;
- inappropriate generated material;
- intellectual property;
- bias; and
- safe and responsible use.

Children should not be encouraged to enter sensitive personal information into public AI systems as part of a Decrypthut activity.

14. SEN, disability and neurodivergence

Decrypthut recognises that children with SEN, disabilities, neurodivergence or communication differences may experience additional barriers to:

- recognising inappropriate behaviour;
- communicating concerns;
- being understood;

- accessing support; or
- being believed.

Staff should take communication and support needs into account when responding to safeguarding concerns.

Behaviour or distress must not automatically be attributed to a diagnosis, disability or additional need.

15. Photography, filming and images

Photography and filming involving children must be managed safely.

Where consent is required for promotional photography or video, appropriate permission must be obtained.

Children who do not have promotional photography permission should, where practicable, be positioned so that they are not identifiable in promotional material.

Staff, contractors and volunteers must not:

- use images of children for personal purposes;
- take unnecessary photographs using personal devices;
- publish children's images on personal accounts; or
- accompany identifiable images with unnecessary personal information.

A child should not be pressured to participate in photography.

Parents, guardians or learners may request that an identifiable promotional image be removed by contacting:

info@decrypthut.com

Decrypthut will stop future use and take reasonable steps to remove the image from digital channels under its control where the relevant consent has been withdrawn.

16. One-to-one working

One-to-one activity must be appropriately managed.

Where possible:

- sessions should occur in observable or appropriately supervised environments;
- another responsible adult should know the session is taking place;
- online sessions should use authorised systems;
- unnecessary private communication should be avoided; and
- appropriate records should be maintained.

The safeguarding arrangements should reflect the child's age, the nature of the programme and the environment in which it is delivered.

17. Missing children, collection and supervision

Where Decrypthut is responsible for supervision or collection arrangements, appropriate procedures must be established before delivery.

A child should only be released in accordance with the agreed collection arrangements applicable to the programme.

If a child cannot be located, staff must act immediately, alert the responsible programme lead and venue, and contact emergency services where necessary.

18. Photography and visitors at events

Parents, visitors, photographers or partner representatives attending Decrypthut activities must comply with venue and programme rules concerning images and safeguarding.

Permission to attend an event does not automatically give permission to photograph or publish images of children.

19. Confidentiality and information sharing

Safeguarding information is confidential but is not secret.

Information should be shared on a need-to-know basis where necessary to safeguard a child or comply with legal responsibilities.

The safety of a child takes priority over a desire to keep information confidential.

20. Record keeping

Safeguarding records should be:

- factual;
- dated;
- appropriately detailed;
- securely stored;
- accessible only to authorised persons; and
- retained in accordance with appropriate safeguarding and legal requirements.

21. Working with schools, councils and partners

Before delivery, Decrypthut will establish appropriate arrangements concerning:

- responsibility for safeguarding;
- relevant DSL contacts;
- emergency procedures;
- attendance;
- collection where applicable;
- first aid;
- photography;
- reporting concerns; and
- relevant learner needs.

When working in a school, Decrypthut personnel must comply with applicable school safeguarding arrangements.

22. Training

People working with children must receive safeguarding information and training appropriate to their role.

Safeguarding forms part of relevant Decrypthut induction and programme preparation.

The DSL should maintain safeguarding knowledge appropriate to the responsibilities of the role.

23. Whistleblowing

Anyone working for Decrypthut who has concerns about unsafe practice, inappropriate behaviour or the way a safeguarding matter has been handled should raise the concern.

No person should suffer retaliation for raising a genuine safeguarding concern in good faith.

Where internal reporting is inappropriate or ineffective, concerns may be raised with an appropriate external safeguarding or statutory body.

24. Review

This policy will be reviewed at least annually and sooner where:

- legislation or guidance materially changes;
- Decrypthut's activities change;
- a safeguarding incident identifies learning;
- a partner or authority requires changes; or
- safeguarding practice indicates that the policy should be strengthened.

Designated Safeguarding Lead: Michaela Carew

Contact: info@decrypthut.com

Policy owner: Decrypthut Limited

Next scheduled review: September 2027

COOKIE POLICY

Decrypthut Limited

Effective date: September 2026

1. About this Cookie Policy

This Cookie Policy explains how Decrypthut Limited (“Decrypthut”, “we”, “us” or “our”) uses cookies and similar technologies when you visit our website.

Decrypthut Limited is registered in England and Wales under company number **13085156**.

Registered office:

**71–75 Shelton Street
London
WC2H 9JQ
United Kingdom**

Email: info@decrypthut.com

This Cookie Policy should be read alongside our Privacy Policy.

2. What are cookies?

Cookies are small files or pieces of information stored on, or accessed from, your computer, smartphone, tablet or other device when you visit a website.

Cookies can perform different functions. For example, they can help a website operate securely, remember preferences or provide information about how visitors use a website.

The rules described in this policy may also apply to similar technologies that store information on or access information from your device, including pixels, tags, scripts, local storage and similar technologies.

In this policy, we use “cookies” as a convenient term for these technologies where appropriate.

3. How we use cookies

Decrypthut may use cookies and similar technologies to:

- operate and secure our website;
- remember your cookie choices and preferences;
- enable website functionality;
- understand how visitors use our website;
- measure and improve website performance;
- support forms and other interactive features;
- display or enable third-party content, where used; and
- identify and resolve technical problems.

We do not use non-essential cookies or similar technologies unless we have an appropriate legal basis to do so.

4. Strictly necessary cookies

Some cookies and technologies are necessary for our website or a service you request to function.

These may be used for purposes such as:

- website security;
- fraud prevention;
- maintaining website sessions;
- load balancing;
- remembering your privacy or cookie preferences;
- enabling a function you have specifically requested; and
- maintaining essential website functionality.

Where the law allows an exemption for these technologies, your consent is not required.

We will only treat a technology as strictly necessary where the applicable legal requirements for that exemption are met.

5. Analytics and website measurement

We may use analytics or website-measurement technologies to understand matters such as:

- how many people visit our website;
- which pages are viewed;
- how visitors navigate the website;
- whether pages are functioning correctly; and
- how the website can be improved.

Where consent is required by law for a particular analytics technology, it will not be activated unless you have given the required consent.

Where applicable law provides an exemption for a particular use of analytics or statistical technologies, we will only rely on that exemption where its requirements are satisfied, including any applicable transparency and objection requirements.

6. Functional technologies

We may use technologies that provide additional website features or remember choices you make.

These could include technologies used to:

- remember website preferences;
- enable enhanced forms or interactive features;
- remember certain user choices; or
- provide enhanced functionality.

Where these technologies require consent, they will remain disabled unless you choose to enable them.

7. Third-party content and services

Our website may use or display services provided by third parties.

These may include, for example:

- video or media players;
- maps;
- forms;
- analytics services;
- website hosting or security services;
- social or professional media features; and
- other embedded digital content.

A third-party service may use its own cookies or similar technologies when its content or functionality is activated.

Where the relevant technology requires your consent, we will take reasonable steps to prevent it from being activated before that consent is obtained.

Third parties may process information in accordance with their own privacy and cookie policies. We encourage you to review those policies where relevant.

8. Your cookie choices

Where consent is required, you will be given a choice about whether to allow optional cookies or similar technologies.

Our website's cookie controls should allow you, as applicable, to:

Accept optional cookies

Reject optional cookies

Manage your preferences

You should be able to refuse optional technologies without losing access to the core content of the Decrypthut website.

We will not treat simply continuing to browse the website as consent where positive consent is legally required.

9. Changing or withdrawing your choices

Where we rely on your consent, you can change your preferences or withdraw that consent.

You can do this through the cookie settings or preference controls made available on our website.

Withdrawing consent does not affect the lawfulness of processing that took place before consent was withdrawn.

You may also be able to delete or block cookies through your browser or device settings.

Please note that blocking strictly necessary technologies may affect the operation of some website features.

10. How long cookies remain on your device

Some cookies are temporary and expire when your browser session ends.

Others may remain on your device for a specified period or until you delete them.

We will not retain or access information through cookies for longer than is reasonably necessary for the relevant purpose.

Where our website uses a cookie-management platform, further information about individual technologies, their providers, purposes and duration may be displayed through the website's cookie settings.

11. Personal information

Some cookies and similar technologies may involve the processing of personal information.

Where they do, that processing is also subject to applicable UK data protection law and our Privacy Policy.

Our Privacy Policy explains how we use personal information, the lawful bases we rely on, who we may share information with and your data protection rights.

12. Children

Decrypthut works with children and young people and recognises that they deserve particular protection in relation to their personal information and use of online services.

We seek to avoid unnecessary tracking or profiling of children through our website.

Where technologies process children's personal information, we will consider the age of users, the nature of the information and the purpose of the technology when determining the appropriate safeguards.

13. Changes to this Cookie Policy

We may update this Cookie Policy when:

- our website changes;
- the technologies used on our website change;
- our service providers change; or
- applicable law or regulatory guidance changes.

The current version will be published on our website with its effective date.

14. Contact us

If you have questions about this Cookie Policy or our use of cookies and similar technologies, contact:

Decrypthut Limited
info@decrypthut.com

71–75 Shelton Street
London
WC2H 9JQ
United Kingdom

Company number: **13085156**

WEBSITE TERMS OF USE

Decrypthut Limited
Effective date: September 2026

1. About these Terms

These Terms of Use (“Terms”) govern your use of the Decrypthut website.

Please read them before using the website.

By using our website, you agree to comply with these Terms. If you do not agree with them, you should not use the website.

These Terms relate to use of our public website. Separate terms, agreements or contractual arrangements may apply when you book, purchase, commission or participate in a Decrypthut programme or service.

2. About Decrypthut

This website is operated by:

Decrypthut Limited
Company number: **13085156**

Registered office:

71–75 Shelton Street
London
WC2H 9JQ
United Kingdom

Email: info@decrypthut.com

Decrypthut provides technology education, training and related programmes and activities, including workshops, courses, roadshows, mentoring, digital skills development, workforce upskilling and other technology learning and innovation activities.

3. Using our website

You may use our website for lawful personal, educational or business purposes.

You must not use the website:

- in breach of applicable law;
- fraudulently or maliciously;
- to introduce viruses, malware or other harmful material;
- to attempt to gain unauthorised access to the website, its servers, systems or data;
- to interfere with the security or operation of the website;
- to impersonate Decrypthut or another person;
- to collect information from the website through unauthorised automated means;
- to infringe our intellectual property or the rights of another person; or
- in a way that could damage Decrypthut, our learners, partners, systems or other website users.

4. Information on our website

We take reasonable care to ensure that information published on our website is accurate and useful.

However, technology, programmes, partnerships and services evolve.

Website content is therefore provided primarily for general information about Decrypthut and should not be treated as a guarantee that a particular:

- programme;
- course;
- technology;
- facilitator;
- partner;
- opportunity;
- delivery format;
- location;
- date; or
- service

will always be available.

We may update, change, suspend or remove website content where reasonably necessary.

Where you enter into a specific agreement with Decrypthut, the terms of that agreement will govern the relevant service.

5. Educational information

Content on our website is not intended to constitute professional, legal, financial, medical or other regulated professional advice.

Descriptions of educational programmes and potential learning outcomes are intended to explain the nature of our work.

Individual learning experiences and outcomes may vary.

Nothing on the website guarantees employment, admission to another educational programme, professional accreditation or a particular career outcome unless we expressly state otherwise.

6. Digital badges and credentials

Decrypthut may issue digital badges or credentials recognising participation, learning, skills, projects or achievement.

Decrypthut currently uses **Sertifier** as a digital credential technology provider.

Decrypthut determines the credentials it awards and what those credentials represent. Sertifier provides technology used to issue, manage, access, share or verify credentials.

A Decrypthut digital badge represents the criteria stated for that particular badge.

Unless expressly stated otherwise, a Decrypthut digital badge is not:

- a regulated qualification;
- a degree;
- a professional licence;
- statutory accreditation; or
- a guarantee of employment or progression.

Digital badges must not be falsified, altered to misrepresent achievement, transferred to another person or otherwise used fraudulently.

Further information is available in our Digital Badge Policy.

7. Intellectual property

Unless otherwise stated, intellectual property rights in the website and original Decrypthut content belong to Decrypthut Limited or are used by us with appropriate permission.

This may include:

- the Decrypthut name and branding;
- written website content;
- graphics and illustrations;
- original photographs and videos;
- programme concepts;
- educational materials;
- curriculum and course content;
- learning resources;
- digital badge artwork;
- programme frameworks;
- methodologies;
- designs; and
- other original content.

You may view and use our public website for ordinary personal, educational or business information purposes.

You must not, without our permission or another lawful basis:

- reproduce substantial parts of our website;
- republish our materials as your own;
- sell or commercially exploit our content;
- copy or reproduce our proprietary learning materials;

- reproduce Decrypthut badges as false credentials;
- modify our materials in a misleading way; or
- use our branding in a way that suggests a relationship, endorsement or partnership that does not exist.

Nothing in these Terms prevents any use permitted by applicable law.

8. Photographs, video and programme imagery

Our website may contain photographs, video and other media showing Decrypthut programmes, activities, learners, staff or partners.

Images are used in accordance with our privacy and safeguarding arrangements and applicable permissions.

You must not extract or reuse identifiable images of children or other learners from our website for unauthorised purposes.

If you appear in an identifiable Decrypthut photograph or recording and wish to raise a concern or request removal from a digital channel under our control, please contact:

info@decrypthut.com

Requests will be handled in accordance with our Privacy Policy and applicable law.

9. Third-party names and intellectual property

Our website may refer to organisations, universities, councils, businesses, technologies, platforms or other third parties.

Their names, logos, trademarks and other intellectual property belong to their respective owners.

A reference to a third party does not, by itself, mean that the organisation endorses Decrypthut or that a formal partnership exists.

Where we describe a partnership, collaboration or other relationship, that description is intended to reflect the relevant relationship accurately.

10. Links to other websites

Our website may contain links to websites or services operated by third parties.

These links may be provided because we believe the information or service may be useful.

We do not control third-party websites and are not responsible for their content, availability, security or privacy practices.

A link does not necessarily constitute an endorsement.

You should review the terms and privacy information of third-party services before using them.

11. Linking to Decrypthut

You may link to publicly available pages on our website provided that you do so fairly and lawfully and do not:

- damage our reputation;
- falsely suggest endorsement or partnership;

- misrepresent your relationship with Decrypthut; or
- present our website or content in a misleading context.

We may ask for a link to be removed where its use is unlawful, misleading or otherwise materially harmful.

12. Website availability and security

We take reasonable steps to maintain the availability and security of our website.

However, we cannot guarantee that the website will always be available without interruption or that it will be completely free from errors, bugs or security vulnerabilities.

We may temporarily restrict or suspend access where reasonably necessary for:

- maintenance;
- security;
- technical updates;
- legal compliance; or
- circumstances outside our reasonable control.

You are responsible for using appropriate security measures on your own device.

13. Our responsibility to you

Nothing in these Terms excludes or limits liability where it would be unlawful to do so.

In particular, nothing excludes or limits liability for:

- death or personal injury caused by negligence;
- fraud or fraudulent misrepresentation; or
- any other liability that cannot legally be excluded.

If you are using the website as a consumer, nothing in these Terms affects your statutory rights.

The public website is provided primarily for general information about Decrypthut. Subject to the rights and liabilities that cannot legally be excluded, we are not responsible for losses caused solely by reasonable reliance on general website information where a separate professional, contractual or programme-specific assessment would reasonably be required.

Separate contractual terms may apply to programmes and services purchased from or commissioned through Decrypthut.

14. Children's use of the website

Decrypthut works with children and young people, but this public website is not intended to encourage children to provide unnecessary personal information.

Children and young people should use registration, communication and programme systems in accordance with the instructions provided for the relevant programme.

Our handling of children's personal information is explained in our Privacy Policy.

Our approach to children's welfare is set out in our Safeguarding and Child Protection Policy.

15. Privacy and cookies

Our **Privacy Policy** explains how we collect, use and protect personal information.

Our **Cookie Policy** explains how we use cookies and similar technologies.

These policies form part of the information governing use of our website.

16. Safeguarding

Decrypthut is committed to safeguarding children and young people participating in our activities.

Our safeguarding principles and procedures are set out in our **Safeguarding and Child Protection Policy**.

If you have a safeguarding concern relating to a Decrypthut activity, please follow the reporting information in that policy.

If a child or another person is in immediate danger, contact the emergency services.

17. Changes to these Terms

We may update these Terms where reasonably necessary, including to reflect changes to:

- our website;
- our services;
- our technology;
- our organisation; or
- applicable legal or regulatory requirements.

The current version will be published on this website with its effective date.

18. Governing law

These Terms and any non-contractual dispute arising from your use of the website are governed by the laws of England and Wales.

If you are a consumer resident elsewhere in the United Kingdom, you may also benefit from mandatory rights and applicable jurisdiction rules in the part of the United Kingdom in which you live.

Nothing in these Terms removes rights that cannot lawfully be excluded.

19. Contact us

If you have questions about these Terms or the Decrypthut website, contact:

Decrypthut Limited
info@decrypthut.com

71–75 Shelton Street
London
WC2H 9JQ
United Kingdom

Company number: **13085156**