

Cybersecurity & Data Protection Policy

1. PURPOSE

At Lil Creative Studio, we take the security of the information entrusted to us seriously.

This policy explains how we approach cybersecurity and protect the data, systems and information we use in our work with clients, collaborators and suppliers.

We see good security as part of responsible design practice. Protecting information helps us maintain trust, deliver reliable work and reduce risk for everyone we work with.

2. SCOPE

This policy applies to the information and systems we use as part of our work, including:

- Client data and project files.
- Internal business information.
- Digital platforms and websites we manage.
- Devices and accounts used for studio work.
- Information shared with freelancers, collaborators and suppliers.

3. OUR APPROACH

We take a practical, proportionate approach to cybersecurity.

We focus on:

- Reducing risk through good systems and habits.
- Keeping processes simple and consistent.
- Using secure, trusted tools and platforms.
- Limiting access to information to those who need it.
- Keeping our systems and knowledge up to date.
- Staying aware of emerging threats and responding appropriately.

4. DATA PROTECTION

We handle personal and confidential information responsibly and in accordance with applicable data protection requirements, including the UK GDPR.

Our approach includes:

- Only collecting information that is necessary for a clear purpose.
- Using information for the purposes for which it was provided.

- Keeping information accurate and up to date where appropriate.
- Protecting information against unauthorised access, loss or misuse.
- Keeping information only for as long as it is needed
- Respecting individuals' rights in relation to their personal data.

5. DATA STORAGE & HANDLING

We use secure, access-controlled systems to store and manage project and business information.

Access to information is limited to people who need it for their role or to deliver the work.

Where we work with freelancers, collaborators or suppliers, information is shared only where necessary and appropriate safeguards are considered.

We do not sell personal data or use client information for purposes unrelated to the work for which it was provided.

Information that is no longer needed is securely deleted or archived in accordance with our retention practices.

6. ACCESS & SECURITY

We reduce risk through access management and secure working practices:

- Strong and unique passwords.
- Password management tools.
- Two-factor authentication.
- Access controls and regular access reviews.
- Secure, password-protected devices.
- Regular software and security updates.

Access to systems is removed when it is no longer required.

7. SECURE WORKING

We take reasonable steps to protect information wherever we work.

This includes keeping devices secure, locking devices when they are not in use, maintaining up-to-date software and taking care when using public or shared networks.

We also remain alert to common cybersecurity risks such as phishing, malware, ransomware and attempts to gain unauthorised access to systems or information.

8. WEBSITE & DIGITAL SECURITY

For websites and digital platforms that we manage, we take appropriate steps to maintain security and reliability.

Depending on the project, this may include:

- Keeping platforms, themes and plugins up to date.
- Using appropriate security and monitoring tools.
- Working with reliable hosting providers.
- Maintaining regular backups.
- Restricting access to website administration and other sensitive systems.
- Security requirements are considered alongside the needs of each individual website and project.

9. SECURITY INCIDENTS & DATA BREACHES

We take security incidents and data breaches seriously and respond promptly.

If an incident occurs, we will take appropriate steps to contain the issue, protect affected information and systems, assess the potential impact and take action to reduce further risk.

Where a personal data breach meets the relevant legal threshold, we will notify the Information Commissioner's Office (ICO) and affected individuals where required by law.

We will also notify affected clients or other relevant organisations where appropriate.

Following a significant incident, we review what happened and use the learning to strengthen our systems and working practices.

10. WORKING WITH CLIENTS & PARTNERS

Good cybersecurity is a shared responsibility.

We work with clients, freelancers and suppliers to maintain secure ways of working. We expect people working with us to take reasonable care when sharing information, using shared systems and managing access to accounts.

Where we identify a security concern relating to information or systems shared with us, we will raise it with the relevant person or organisation.

11. RESPONSIBILITIES

The Studio Lead has overall responsibility for cybersecurity and data protection within Lil Creative Studio.

Everyone working with us has a responsibility to follow appropriate security practices, protect the information they have access to and report suspected security incidents promptly.

Our suppliers and service providers are selected and managed with consideration given to appropriate security and data protection requirements.

12. CONTINUOUS IMPROVEMENT

Cybersecurity is an ongoing responsibility.

We regularly review our tools, systems and working practices to ensure they remain appropriate and proportionate to the risks we face.

We keep our approach under review as technology, threats, legislation and the way we work evolve.

13. COMMITMENT

We believe that protecting data is part of responsible, ethical design practice.

Good security protects people, builds trust, and supports long-term, sustainable work.

We are committed to continually improving how we protect the information entrusted to us.

POLICY REVIEW

This policy will be reviewed periodically and may be updated to reflect changes in legislation, best practice, organisational priorities or the way Lil Creative Studio operates.

Last updated September 2026