GENIUSCRAFT LTD TRADING AS YOUNG ENGINEERS CANTERBURY

DATA PROTECTION POLICY

Policy statement

Geniuscraft Ltd trading as Young Engineers Canterbury is committed to protecting personal information and handling it lawfully, fairly, transparently and securely across all business activities.

1. Purpose, scope and legal framework

Geniuscraft Ltd trading as Young Engineers Canterbury is committed to protecting personal information about children, parents/carers, employees, volunteers, applicants, suppliers and partners. We process information to deliver safe and inclusive STEM clubs, engineering sessions, workshops, holiday activities and other programmes; manage bookings; meet safeguarding responsibilities; and fulfil legal and contractual duties.

This policy applies to personal data processed in paper, electronic, image, audio or other form by or on behalf of the organisation. It should be read alongside the Safeguarding Policy, privacy notices, image-use procedure, record-keeping and retention schedule, information-sharing procedure and data-breach procedure.

The organisation will comply with the UK GDPR, Data Protection Act 2018, the Data (Use and Access) Act 2025 where applicable, and relevant Information Commissioner's Office (ICO) guidance. This policy does not replace tailored privacy notices or the need to document lawful bases and retention periods for specific processing.

2. Responsibilities

The Director, Tania Prisacariu, is the designated Data Protection Lead and is responsible for implementing this policy, handling rights requests and coordinating breach response. The organisation does not describe this role as a statutory Data Protection Officer (DPO) unless it has formally appointed a DPO and the legal requirements for that role are met.

Staff and contractors must follow this policy, access only information needed for their duties, keep personal information confidential, and report suspected incidents immediately.

Managers or designated staff are responsible for applying the policy in day-to-day operations, collecting and maintaining accurate records, ensuring appropriate access controls, and promptly forwarding data rights requests and suspected breaches to the Data Protection Lead.

3. Data protection principles

- Lawfulness, fairness and transparency: explain what information is collected and why.
- Purpose limitation: use information only for specified, legitimate purposes unless further use is lawful.
- Data minimisation: collect and share only what is necessary.
- Accuracy: take reasonable steps to keep information accurate and correct errors.
- Storage limitation: keep information no longer than necessary under the retention schedule, legal duties and relevant safeguarding, claim or insurance needs.
- Integrity and confidentiality: protect information against unauthorised access, loss, alteration or disclosure.
- Accountability: maintain records and be able to demonstrate compliance.

4. Types of information and purposes

Information may include children's names and dates of birth; attendance and authorised collection arrangements; parent/carer and emergency contact details; allergies, dietary requirements, medical needs and SEND/accessibility information; safeguarding and incident records; photographs and video; payment and booking information; and staff recruitment, DBS-check, training, payroll and employment records. Supplier, venue, school, commissioner and partner contact details may also be processed.

Use information only for legitimate organisational purposes, such as administering bookings, communicating with families, planning safe and inclusive activities, supervising children, responding to emergencies, managing safeguarding concerns, processing payments, managing employment, meeting legal or contractual requirements, and reporting to authorities where required.

5. Lawful bases and special category information

For each processing purpose, the organisation must identify and document an appropriate lawful basis under Article 6 UK GDPR, such as contract, legal obligation, legitimate interests, consent or vital interests, as appropriate to the circumstances. Consent is not the default basis for every activity and must be freely given, specific, informed and withdrawable where consent is relied upon.

Health information, allergies, disability/SEND information and other special category data require both an Article 6 lawful basis and an applicable Article 9 condition. Where required, a condition under the Data Protection Act 2018 and an appropriate policy document must also be in place. Information must be limited to what is needed to keep a child safe and support participation.

6. Privacy information and children's data

Provide parents/carers and staff with clear privacy information explaining what data is collected, purposes, lawful bases, recipients, retention, rights and how to contact the organisation.

Explain information in a clear, age-appropriate way to children where appropriate, taking particular care because children may not fully understand how their information is used.

Use separate, clear choices for public marketing images and other optional uses. Booking or attendance consent must not be treated as automatic permission to publish images.

Keep a record of image permissions and restrictions. Do not publish identifiable images where permission or another lawful basis is absent, unclear or withdrawn, and follow any safeguarding restriction.

7. Sharing information

Personal data may be shared only when necessary, proportionate and lawful. Depending on the purpose, recipients may include parents/carers, the host school or venue, commissioners, emergency services, children's social care, police, safeguarding agencies, insurers, booking/payment providers, IT/cloud providers, payroll providers and professional advisers.

Safeguarding information may be shared without consent where there is a lawful basis and sharing is necessary to protect a child or another person. Staff must not promise absolute confidentiality.

Share the minimum necessary information, with the right recipient, using an appropriate secure method. Record significant safeguarding information-sharing decisions and the rationale. If unsure, seek advice promptly from the DSL/Director, but do not delay urgent protective action.

8. Security and authorised access

Keep paper records in locked storage and transport them securely. Do not leave registers, medical/allergy information or safeguarding records visible to other families or visitors.

Use organisation-approved accounts, devices, cloud systems and booking platforms with suitable access controls, strong passwords and multi-factor authentication where available.

Limit access by role and review permissions when staff join, change roles or leave. Do not share passwords or use another person's account.

Check recipients and attachments before sending email; use secure sharing for sensitive information. Do not use personal email, personal cloud storage or unapproved messaging for personal data unless expressly authorised under a documented secure arrangement.

Keep devices updated, lock screens when unattended, and report lost devices, misdirected messages, unauthorised access or suspicious activity immediately.

Use suppliers and processors with appropriate security and contractual protections. Where required, put a data-processing agreement in place and assess international transfers before they occur.

9. Data breaches and incident response

Any staff member who suspects a loss, misdirection, unauthorised access, alteration, disclosure or destruction of personal data must report it immediately to the Director/Data Protection Lead. Do not wait to establish whether harm occurred.

The Director/Data Protection Lead will take reasonable steps to contain the incident, preserve evidence, assess the type and volume of data, people affected, likely consequences and actions needed to reduce harm. Record the facts, effects, containment, risk assessment, decisions and remedial actions in a breach log, including incidents that are not reportable to the ICO.

Where a personal data breach is likely to result in a risk to people's rights and freedoms, notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. If notification is later, document the reasons.

Where the breach is likely to result in a high risk to people's rights and freedoms, inform affected individuals without undue delay unless a legal exception applies.

Notify a venue, commissioner, insurer, service provider or other party where required by law, contract or the circumstances.

10. Individual rights and requests

Individuals may have rights to access their data, rectify inaccuracies, erase data in certain circumstances, restrict or object to processing, receive portable data where applicable, and withdraw consent where consent is the basis. Rights are not absolute and some information may be retained or withheld where a lawful exemption applies, including where disclosure would prejudice safeguarding or another person's rights.

Requests may be made verbally or in writing. Staff must forward them promptly to the Director/Data Protection Lead and must not respond informally by disclosing records.

The organisation will verify identity proportionately, log the request and respond within the applicable statutory period, normally one month, subject to lawful extensions or exemptions. No fee is normally charged.

11. Retention and secure disposal

The organisation will maintain a retention schedule for booking and attendance records, finance and tax records, recruitment and employment records, DBS information, medical/allergy information, accident records, safeguarding records, images and contractual records.

Retention periods must be based on legal obligations, safeguarding needs, limitation periods, contractual requirements and insurance requirements—not a blanket period applied to every record. The organisation will not apply a fixed retention period to all children's or staff records without checking the relevant purpose and requirements.

When the retention period ends, records must be securely shredded, securely deleted or irreversibly anonymised. Backups and supplier systems should be considered as part of disposal arrangements. A legal hold, safeguarding concern or active claim may justify longer retention where documented and lawful.

12. Data protection by design and risk assessment

Before introducing new systems, collecting new categories of information, using new technology, sharing data at scale or processing sensitive information in a way that may create high risk, the Director will consider privacy risks and whether a Data Protection Impact Assessment (DPIA) is required. Collect only the data needed and build privacy and access controls into the process.

13. Training, monitoring and complaints

Staff and volunteers receive role-appropriate data protection and confidentiality induction, including safeguarding information-sharing, image use, secure communication and breach reporting.

The Director will monitor compliance, investigate concerns and review this policy after incidents or changes to processing. Individuals may raise concerns with the Director/Data Protection Lead or complain to the Information Commissioner's Office (ICO).

14. Relevant guidance and related documents

This policy should be read with the organisation's Safeguarding Policy, privacy notices, image-use procedure, information-sharing procedure, data-breach procedure, record-keeping and retention schedule, and relevant staff guidance.

UK GDPR and Data Protection Act 2018: https://www.legislation.gov.uk/eur/2016/679/contents

Data Protection Act 2018: https://www.legislation.gov.uk/ukpga/2018/12/contents

Information Commissioner's Office — children and the UK GDPR: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/

Information Commissioner's Office — personal data breaches: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

Data (Use and Access) Act 2025: https://www.legislation.gov.uk/ukpga/2025/18/contents

15. Review and document control

This policy will be reviewed at least annually and sooner after a significant incident, a change in activities or systems, or a relevant change in law, guidance or contractual requirements.

Approval

Policy owner	Director
Approved by	Tania Prisacariu, Director
Approval date	25/10/2026
Next review date	25/09/2027