Information Governance Policy

School of Dough CIC
Version: v1 **Approved by:** Francesco Rigolli, Matthew Comley **Date:** 17/12/2025
Policy Owner: Francesco Rigolli
Next Review Due: [16/12/2026

Scope: This policy applies to all directors, staff, volunteers, and partners handling information for School of Dough CIC, including information relating to **children and young people** who attend our cooking classes, their parents/guardians, and our personnel.

1. Purpose

This policy sets out how School of Dough CIC manages information lawfully, securely, and ethically, in line with:

- **UK GDPR** and the **Data Protection Act 2018**
- **PECR** (for electronic communications such as email/text marketing)
- **Safeguarding** duties for children and young people
- Relevant sector guidance

Our aims are to protect the rights and freedoms of individuals, support safe and effective service delivery, and maintain public trust.

2. Roles & Responsibilities

- **Directors**: Accountable for compliance and resource allocation.
- **Senior Responsible Owner (SRO)**: Francesco Rigolli – ensures this policy is implemented.
- **Data Protection Lead (DPL)**: Francesco Rigolli (director), schoolofdoughcic@gmail.com – day-to-day compliance, advice, DPIAs, breaches, rights requests, records.
- **Safeguarding Lead (DSL)**: – Francesco Rigolli (director), schoolofdoughcic@gmail.com, manages safeguarding concerns and lawful information sharing.
- **All Staff & Volunteers**: Must complete training, follow this policy and report incidents quickly.
- **Processors / Service Providers**: Must have contracts with data protection clauses and be vetted.

*The DPL fulfils advisory and monitoring duties.

3. Data We Process

We process personal data to run cooking classes, ensure safety, and manage our CIC.

3.1 Participant Data (Children & Young People)

- **Identity & Contact:** name, age when first registering, parent/guardian contact details
- **Attendance & Progress:** registrations, attendance logs, session notes
- **Health & Safety:** allergies, dietary requirements, medical information necessary for safe participation, incidents/accidents
- **Images/Media:** photos/video (only with explicit consent)
- **Safeguarding:** records of concerns, referrals, and outcomes (restricted access)

3.2 Parent/Guardian & Carer Data

- Contact details, consent records, communications, payment details (when applicable)

3.3 Staff & Volunteers

- Recruitment records, DBS checks, training, rota/attendance, emergency contacts

3.4 Supporters / Funders / Partners

- Contact details, grant or reporting information, feedback, impact measurement

4. Lawful Bases & Special Category Data

We rely on the following lawful bases:

- **Contract** – to deliver booked classes to participants/parents
- **Legal obligation** – safeguarding, health & safety, accident reporting, HMRC
- **Vital interests** – sharing relevant data in emergencies (e.g., with paramedics)
- **Public task / Legitimate interests** – service administration, improvement, impact reporting (use Legitimate Interests Assessment (LIA) where appropriate)
- **Consent** – strictly for **optional** activities like photography/media and certain communications

Special Category Data (e.g., health, dietary requirements) is processed under:

- **UK GDPR Art. 9(2)(a)** (explicit consent) for non-essential health info; and/or
- **Art. 9(2)(c)** vital interests (where consent cannot be given)
- **Art. 9(2)(g)/(h)** where applicable for safeguarding/health purposes and with appropriate safeguards.

Children's Consent: For **information society services**, the UK age for child consent is **13**. For our classes, parental/guardian consent is required where appropriate. We ensure consent is **freely given, specific, informed, and revocable**.

5. Data Minimisation & Purpose Limitation

- Collect only what is necessary (e.g., **allergy details needed to keep a child safe during sessions**, not full medical histories).
- Use data only for the stated purposes.
- Regularly review forms and systems to remove unnecessary fields.

6. Transparency (Privacy Notices)

We provide clear privacy notices to:

- **Participants & Parents/Guardians** at sign-up
- **Staff/Volunteers** during onboarding
- **Supporters/Donors** during subscription/donation

Notices include: controller details, purposes, lawful bases, retention, sharing, rights, complaints (ICO), and contact details. We use **age-appropriate language** and accessible formats.

7. Individual Rights Handling

We uphold rights of access, rectification, erasure, restriction, objection, portability, and rights related to automated decision-making.

- **Requests to:** Francesco Rigolli (director), schoolofdoughcic@gmail.com / 07553384523 / 16 Fore St, St Dennis, PL26 8AF.
- **Verification:** Confirm identity and authority (for parents/guardians).
- **Timescales:** Normally within **one month**.
- **Safeguarding Records:** Erasure and access may be limited where necessary to protect a child or ongoing investigations; we document the legal basis for any limitation.

Appendix B contains a standard **Subject Access Request (SAR)** workflow and response templates.

8. Data Sharing

We may share data with:

- **Emergency services** (vital interests)
- **Safeguarding partners** (e.g., local authority, police) where necessary and lawful
- **Funders** (aggregated/anonymised wherever possible)
- **Service providers** (IT, scheduling, payment processors, email providers) under **Data Processing Agreements (DPAs)**

Before sharing: confirm lawful basis, necessity, proportionality, and security. Prefer anonymised/pseudonymised data for monitoring and impact reporting.

9. Processors & Due Diligence

We only use processors that provide sufficient guarantees of security and compliance. For each processor we maintain:

- **Purpose & data types processed**
- **Contract with UK GDPR clauses** (confidentiality, sub-processors, security, breach notification, deletion/return on termination)
- **Location of data** (UK), transfer safeguards
- **Security posture** (encryption, access controls, certifications)
- **Retention and deletion commitments**

Appendix C includes a **Processor Register template**.

10. Information Security

10.1 Access Control

- **Least privilege** access to systems and safeguarding records
- Named accounts, strong passwords, MFA where available
- Joiners/movers/leavers access reviews

10.2 Devices & Storage

- Approved devices only; **no sharing** of logins
- Full-disk encryption on laptops/phones used for CIC work
- **No local storage** of sensitive data unless necessary and encrypted
- **Secure, limited-access** storage for safeguarding files

10.3 Communications & Collaboration

- Use approved email and messaging channels
- **No participant data** in unsecured messaging apps; if WhatsApp is used for logistics, avoid sensitive data and enable device security
- Password-protect and encrypt attachments with separate password channels
- Verify recipients before sending

10.4 Physical Security

- Lockable cabinets for any paper files
- Clean desk policy for events/classes
- Secure transport of registers and consent forms to/from venues

11. Children's Safety & Safeguarding Data

- **Safeguarding Lead** manages and restricts access to safeguarding information
- **Record keeping:** factual, necessary, accurate, dated, with clear actions and outcomes
- **Information sharing:** lawful, proportionate, and documented (who, what, why, lawful basis)
- **DBS checks:** required for eligible roles; records kept minimally (status/date, not full certificate copies)
- **Incidents/accidents:** recorded with retention per schedule

12. Photography, Video, and Marketing

- **Explicit, informed consent** from parent/guardian or competent young person before any photography/video
- Provide **opt-in** checkboxes separately from service terms
- Respect **no-photo** preferences operationally (badges, lists, briefing staff/volunteers)
- For marketing emails/SMS: comply with **PECR**; obtain opt-in where required and provide easy **unsubscribe**
- Avoid naming children in posts; use first names only (or anonymise) and never pair names with identifiable locations/times without necessity and consent.

13. Data Retention & Disposal

We retain data **no longer than necessary**. Standard retention (customise in Appendix D):

- **Participant registration & consent:** current year + **3 years**
- **Safeguarding records: until the child turns 25** or longer if required by guidance (check local safeguarding guidance)
- **Accident/incident reports: 3–7 years** depending on severity/insurance
- **Medical/allergy info:** retained only while necessary for safe participation
- **Photography consent records:** as long as the media is stored/used
- **HR/Volunteer records:** typically **6 years** after leaving (limited DBS metadata for **up to 6 months**; do not store full certificates)
- **Finance (incl. donations): 6 years** for HMRC

Secure disposal: cross-cut shredding for paper; cryptographic wipe or secure deletion for electronic files; deletion certificates from processors on contract end.

14. Data Breach Management

A **personal data breach** includes loss, unauthorised access/disclosure, or alteration.
All staff/volunteers must report within 24 hours to the DPL.

Process:

1. **Contain** the breach and secure systems
2. **Assess risk** to individuals (harm, sensitivity, volume, special category data)
3. **Decide on ICO notification** within **72 hours** if risk is likely to rights/freedoms
4. **Inform affected individuals** if high risk, with advice and contacts
5. **Document** in the **Breach Log** (Appendix E) and implement lessons learned

15. Data Protection Impact Assessments (DPIAs)

We conduct DPIAs where processing is likely to result in **high risk**, including:

- New apps/systems for managing children's data
- Systematic monitoring (e.g., CCTV in class areas)
- Large-scale processing of special category data (health)
- Innovative tech or profiling

The DPIA includes purpose, necessity/proportionality, risks, mitigations, and consultation where appropriate.

16. Training & Awareness

- **Induction training** for all staff/volunteers before handling data
- **Annual refreshers** and ad-hoc updates for changes in law/process
- Keep **training records**

17. Records of Processing Activities (ROPA)

We keep a ROPA (Appendix A) covering:

- Purposes
- Categories of data subjects and personal data
- Recipients
- Retention
- Technical and organisational security measures

18. Audit, Monitoring & Review

- Annual review of this policy and supporting procedures
- Spot checks on access controls, retention, and processors
- Report findings to the Board/Directors with remedial actions

20. Contact & Complaints

Data Protection Lead: Francesco Rigolli (director), schoolofdoughcic@gmail.com
Safeguarding Lead: Francesco Rigolli (director), schoolofdoughcic@gmail.com
Postal Address: 16 Fore St, St Dennis, PL26 8AF
Complaints: We aim to resolve issues promptly. Individuals may also complain to the **Information Commissioner's Office (ICO)**.

Appendices (Templates & Checklists)

Appendix A – ROPA (Register of Processing Activities)

Processing Activity	Purpose	Data Subjects	Data Categories	Lawful Basis	Special Category Basis	Recipients/Processors	Retention	Security
Class registration & attendance	Manage enrolment & attendance	Children; Parents	Names, age when registering, contacts	Contract/LI	N/A	[Scheduling app]	Current + 3 yrs	MFA, encryption
Health & allergies	Ensure safety in sessions	Children	Health, dietary	Consent/Vital Interests	Art. 9(2)(a)/(c)	Staff; first aiders	Active participation only	Need-to-know access
Safeguarding	Protect children	Children; families	Safeguarding notes	Legal obligation/Public task/LI	Art. 9(2)(g)/(h)	LA, Police	Until age 25 (min)	Restricted store
Photos & media	Marketing & reporting	Children	Images	Consent	N/A	Website/social	As long as in use	Consent ledger
HR/Volunteers	Admin & compliance	Staff/Vols	IDs, checks	Legal obligation/Contract	N/A	Payroll/DBS	6 yrs post-leaver	Role-based access

Replace [LI] with Legitimate Interests and complete Transfer safeguards where applicable.

Appendix B – Rights Requests (SAR) Workflow

1. Receive request at [privacy@…] → log date/time.
2. Verify identity/authority (parent/guardian if applicable).
3. Clarify scope (date range, categories).
4. Search systems (email, cloud storage, apps, paper).
5. Review & redact third-party data and safeguarding sensitivities.
6. Respond **within one month** (extensions in complex cases documented).
7. Record in **Rights Requests Log**.

SAR Response Template:

- What we hold, why, sources, recipients, retention, rights, complaint to ICO, copy of data (secure channel), reasons for any redactions/limitations.

Appendix C – Processor Register & Due Diligence

Provider	Service	Data	UK/EEA Location	Contract/DPA	Security (MFA/Encryption)	Sub-processors	Deletion on Exit
[Example: Acme Schedules]	Class bookings	Names, emails	UK	DPA signed	MFA, TLS	Listed	Yes

Checklist: data location, breach notification, access controls, backups, vulnerability management, certifications (e.g., Cyber Essentials), audit rights.

Appendix D – Retention Schedule (Customise)

Record Type	Retention	Rationale
Registrations & attendance	Current year + 3 yrs	Service records/queries
Allergy/medical notes	While active + review annually	Safety necessity only
Accident/incident	3–7 yrs (severity dependent)	Insurance/legal
Safeguarding	Until child turns 25 (min)	Sector guidance
Photos/media + consent	While in use; review annually	Consent-based
HR/Volunteer files	6 yrs post-leaver	Limitation periods
DBS metadata (status/date)	Up to 6 months	ICO guidance
Finance (incl. donations)	6 yrs	HMRC

Appendix E – Data Breach Log

Date/Time	Reporter	Description	Data Types	Individuals Affected	Risk Level	Actions Taken	MARU Notified?	Individuals Notified?	Lessons Learned

Appendix F – Consent Forms (Key Fields)

- Participant name; parent/guardian details; session(s)
- Specific consents (tick boxes):
  - □ Emergency medical information sharing (vital interests)
  - □ Photo/video for **website/social**
  - □ Photo/video for **funders/reports**
  - □ Email/SMS about **future classes/events** (marketing)
- Clear explanation, ability to **withdraw consent** at any time, contact details, date/signature.

Appendix G – Classroom/Session Data Handling SOP

- Bring **only** the day's register, allergy list, and emergency contacts.
- Keep papers secured and **out of public view**.
- Brief staff on **no-photo** list at start of session.
- After session: return papers to office or **securely store**; upload updates to system; **shred** obsolete copies.
- Report any **incidents or near misses** to the DPL and DSL.

Appendix H – BYOD & Messaging Quick Rules

- Devices must have **screen lock**, **auto-lock**, **encryption**, and **up-to-date OS**.
- Do not store participant lists in personal photo galleries or unencrypted notes.
- Use only approved apps/email; avoid discussing sensitive data in group chats.
- If a device is lost/stolen: **report immediately**; enable remote wipe if possible.

Policy Acceptance

I confirm I have read and will comply with this policy:

Name: _____
Role: _____
Signature: _____ **Date:** _____

Customisation Notes (for you)

*Safeguarding contact MARU: multiagencyreferralunit@cornwall.gov.uk - 0300 123 1116

- If you publish privacy notices on your website, keep URLs in Section 6.