

DATA PROTECTION POLICY

BREACH PROCEDURE & DPIA

2026

**Data Protection Policy, Breach
Procedure & DPIA**

Version 2.0

**STEM
ON TRACK**

INTRODUCTION

At STEM On Track, operated by Espire Education, we are committed to safeguarding your personal data in compliance with the UK Data Protection Act 2018 and UK GDPR. This Data Protection Policy outlines how we collect, use, store, and protect personal information, as well as your rights as a data subject. As the data controller, Espire Education ensures that all personal data is processed lawfully, transparently, and securely.

ADAM SIRETT

Email: adam@espireeducation.co.uk

Phone: 07814 274241

JAMES FOSTER LE-GRYS

Acting *Data Protection Officer (DPO)*

Email: james@espireeducation.co.uk

Phone: 07585 721939

DATA PROTECTION POLICY

1. POLICY OVERVIEW

This policy applies to all personal data collected through the STEM On Track programme, including our website, the Race Academy platform, and race day activities. We collect and process personal data only as necessary for programme administration, communication, and compliance with legal obligations, ensuring robust security measures and respect for your privacy.

2. DATA COLLECTION AND PURPOSE

We collect personal data directly from schools, teachers, and students to facilitate the STEM On Track programme. The data we collect includes:

- **Teachers:** Names, email addresses, postal delivery addresses, and finance team contact details to manage programme participation, provide updates, and coordinate communications.
- **Students (Necessary for Participation):** Names and email addresses and date of birth for participation and creation of logins for the Race Academy platform, and compliance with health & safety, and insurance purposes for on-track events.
- **Students (Optional Consent-based):** Gender, year group, ethnicity, a driver medical/fitness declaration, and photographs for marketing. We process special category data (ethnicity and health) with explicit consent.

2.1 Purposes of Data Collection:

- **Service Delivery:** To provide access to the Race Academy platform for educational content and resources.
- **Event Management:** To ensure safety and compliance with insurance requirements during race day activities.
- **Driver Safety:** Where a student takes part as a driver, to confirm through a fitness declaration that they are medically able to do so safely, for safety and insurance purposes.

- **Character Personalisation:** To enable a student, with explicit parental consent, to create an on-screen character that reflects them, using the ethnicity information provided.
- **Equality, Diversity and Inclusion (EDI) Monitoring:** To understand and improve the diversity of the students we work with and ensure the programme reflects the communities we support. EDI information is reviewed only in anonymised, aggregated form (for example, how many participants are of a given ethnicity) and never to identify individuals; it also supports our social impact (SROI) reporting.
- **Communication:** To share programme updates, event details, and administrative information with teachers and schools.
- **Marketing and Promotion:** To promote the programme using photographs that may include students, where consent has been given.

3. LAWFUL BASIS FOR PROCESSING

Lawful Basis:

- **Consent:** For marketing (e.g., newsletters, photographs), explicit consent is obtained from the parent/guardian, withdrawable at any time via info@espireeducation.co.uk.
- **Legitimate Interest:** For essential programme administration, including platform access, school communication, and management of necessary participation data (name, school email, date of birth).
- **Legal Obligation:** For race day insurance/safety compliance.
- **Explicit Consent (Art. 9(2)(a)):** For special category data — ethnicity (used for character personalisation) and the driver medical/fitness declaration — explicit parental consent is obtained, in addition to the Article 6 basis above. Special category data requires both an Article 6 lawful basis and an Article 9 condition; legitimate interest alone is not sufficient.
- **Equality Condition (DPA 2018, Sch. 1, Pt. 2, para. 8):** For aggregate EDI/diversity monitoring, processing also relies on the equality-of-opportunity condition. Reliance on this condition requires an Appropriate Policy Document to be maintained, covering compliance with the data-protection principles and our retention and erasure approach for this data.

Data Minimisation: Date of birth, rather than age alone, is collected because it is necessary to apply the age-13 consent threshold accurately and to verify driver eligibility against a fixed date (drivers must be 16 or under by 1 June 2027). No other purpose relies on date of birth, and it is not used for any other decision about a student.

Consent Gating: Optional and special category data (EDI, the driver declaration, photographs) is collected only where the corresponding parental consent has been recorded, enforced through the platform design rather than relying on supervision. A student whose parent has not given a particular consent is routed to the generic equivalent of that feature (for example, a freely designed character with no ethnicity recorded) and is not denied access to the programme. Participation is never conditional on giving any optional or special category consent.

5. DATA STORAGE AND SECURITY

All personal data is stored securely on Google Cloud and AWS platforms, hosted within the UK and EEA, ensuring compliance with UK GDPR. These platforms adhere to industry-standard security protocols, including:

- **Encryption:** Data is encrypted in transit and at rest.
- **Access Controls:** Data is stored in password-protected folders, accessible only by two authorised Espire Education staff members managing the Race Academy platform.
- **Compliance Standards:** Google Cloud and AWS comply with ISO 27001, SOC 2, and other certifications. For details, see Google Cloud Privacy Notice and AWS Privacy & Security.
- **Special Category Data:** Stored only where consent is recorded, and that aggregate reporting is anonymised with small cell counts suppressed.

No data is transferred outside the UK/EEA, eliminating the need for additional data transfer mechanisms like Standard Contractual Clauses (SCCs).

4. THIRD-PARTY DATA ACCESS

Personal data is primarily managed by Espire Education. Limited access may be granted to:

Marca Media: Our UK-based (Manchester) technical partner for the Race Academy platform. Only two authorised staff members may access data for troubleshooting technical issues. Marca Media does not collect, store, or retain personal data.

Hosting Circuits (e.g. Whilton Mill, Silverstone etc.): No personal data is shared with the hosting circuit. Race day safety and insurance compliance are managed directly by Espire Education.

Private Paramedics (e.g. MediTechGlobal): On-site medical providers may access a driver's fitness-to-drive declaration in the event of a medical emergency during race day activities. This is limited to drivers whose parent/guardian has given explicit consent to the driver medical declaration, and access is restricted to what is necessary to respond to the emergency.

Event Management Agency: As appropriate, for the operational delivery of events. No special category data is shared for marketing or with other third parties without explicit consent.

No personal data is shared with other third parties unless required by law or with your explicit consent.

6. AGE RESTRICTIONS AND PARENTAL CONSENT

The STEM On Track programme is primarily designed for students aged 11 to 16. Students over 16 may also participate, provided they are not taking part as drivers; the driver role is restricted to those aged 16 or under (by 1 June 2027, see Section 2.1). For all participants under 13, we require parental consent, obtained through our online platform, before processing any of their personal data. In line with our data protection policy and terms of engagement, the teacher provides the student's school email and the parent's email; the parent completes an online tickbox consent; consent is logged (Art. 7).

For all participants, regardless of age, separate explicit parental consent is required before we process any optional or special category data — specifically gender, year group, ethnicity, the driver medical/fitness declaration, and photographs for marketing. This consent is sought in addition to, and is distinct from, the under-13 consent described above, and applies equally to students aged 13 and over.

7. DATA RETENTION

We retain personal data only as long as necessary for the purposes outlined in this policy or as required by law:

Teacher Data: Retained for the duration of the school's participation in the programme, plus 3 months for administrative purposes, unless otherwise requested.

Student Data: Retained for the academic year of participation, plus 3 months, to support programme continuity and compliance.

EDI Data (ethnicity, gender, year group): Where provided with explicit parental consent, identifiable EDI data is retained for the same period as the associated student record (academic year of participation, plus 3 months) or until consent is withdrawn, whichever is earlier. Once anonymised and aggregated for diversity monitoring and SROI reporting, this data is no longer personal data and may be retained indefinitely.

Driver Medical Declaration: The completed medical declaration form, including the underlying medical information provided, is retained until the National Finals race event (e.g. 18th June) and then securely deleted, including from backups, within 30 days of that period ending.

Marketing Photographs: Retained only while consent subsists. On withdrawal of consent, photographs are removed from future use; materials already printed or published before withdrawal cannot always be recalled.

Backups: Backups and archival copies are removed within 30 days of the end of the relevant retention period above, or upon a valid deletion request

8. DATA DELETION PROCESS

When personal data is no longer needed, it is securely deleted from Google Cloud and AWS. Backups and archival data are removed within 30 days of the retention period's end or upon request. You may request deletion of your data at any time by contacting info@espireeducation.co.uk.

9. YOUR DATA PROTECTION RIGHTS

Under UK GDPR, you have the following rights:

- Right to Access: Request a copy of your personal data.
- Right to Rectification: Correct inaccurate data.
- Right to Erasure: Request deletion of your data, subject to legal obligations.
- Right to Restriction: Restrict processing under certain conditions.
- Right to Object: Object to processing based on legitimate interest.
- Right to Data Portability: Request your data in a structured, machine-readable format.
- Right to Withdraw Consent: Where we rely on consent, you may withdraw it at any time; this will not affect anything done beforehand.
- Right to Complain to the ICO: If you are unhappy with how we have handled your personal data, you have the right to complain to the Information Commissioner's Office (ICO) at ico.org.uk.

To exercise any of the rights above or raise concerns, contact us at info@espireeducation.co.uk.

10. POLICY UPDATES

We may update this policy to reflect changes in our practices or legal requirements. Significant updates will be communicated via our website and, where necessary, directly to affected parties.

11. CONTACT INFORMATION

For questions, concerns, or to exercise your data protection rights, please contact:

- General Enquiries: support@espireeducation.co.uk
- Acting DPO: info@espireeducation.co.uk
- Management: adam@espireeducation.co.uk



STEM ON TRACK DATA BREACH PROCEDURE

DATA BREACH PROCEDURE

Version: 1.0

Date: June 2026

Owner: Acting Data Protection Officer (James Foster Le-Grys)

Approved By: Director (Adam Sirett)

1. PURPOSE AND SCOPE

This procedure sets out how Espire Education Group Limited identifies, manages, and reports personal data breaches in line with Articles 33 and 34 UK GDPR. It applies to all staff, contractors, and processors handling personal data for the STEM On Track programme.

2. WHAT IS A PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It covers three types of incident:

- Availability — loss of access to, or destruction of, personal data (availability);
- Integrity — unauthorised or accidental alteration of personal data (integrity);
- Confidentiality — unauthorised disclosure of, or access to, personal data (confidentiality).

Examples relevant to STEM On Track: an email containing student details sent to the wrong recipient; a lost or stolen device with access to the platform; unauthorised access to Google Cloud/AWS; ethnicity or driver-health data exposed; or a processor (e.g. Marca Media) reporting an incident.

3. ROLES AND RESPONSIBILITIES

- **All staff/contractors** — report any suspected or actual breach immediately and do not attempt to investigate or resolve it alone.
- **Acting DPO** — coordinates the response, assesses risk, decides on ICO and individual notification, and maintains the breach register.
- **Director** — approves notifications and any external communications, and authorises remedial spend.
- **Processors** — must notify Espire without undue delay on becoming aware of a breach affecting Espire data, under their contract.

4. THE RESPONSE STEPS

Step 1 — Identify and report (immediately)

Any individual who becomes aware of a suspected breach reports it to the DPO immediately, and at the latest within 24 hours of discovery, using the internal breach report form (Appendix A). Early reporting is essential because the ICO clock (Step 4) is short.

Step 2 — Contain and recover

The DPO, with relevant staff and processors, takes immediate steps to contain the breach (e.g. revoke access, recall or delete misdirected data, reset credentials, isolate systems) and to recover any lost data. Preserve evidence and a timeline of events.

Step 3 — Assess the risk

The DPO assesses the risk to individuals' rights and freedoms, considering the type and sensitivity of data, the number of individuals, the ease of identification, and the severity of consequences. The involvement of children and of special category data (ethnicity, health) raises the risk and weighs in favour of notification. The assessment is recorded.

Step 4 — Notify the ICO (within 72 hours)

Where the breach is likely to result in a risk to individuals' rights and freedoms, the DPO notifies the ICO without undue delay and within 72 hours of Espire becoming aware. The notification describes the nature of the breach, the categories and approximate number of individuals and records affected, the likely consequences, the measures taken, and the DPO contact. If notification is made after 72 hours, the reasons for delay are given. If no notification is made, the justification is recorded.

Step 5 — Notify affected individuals

Where the breach is likely to result in a high risk to individuals, the DPO informs the affected individuals (for children, their parents/guardians) without undue delay, in clear, plain language, describing the breach, the likely consequences, the measures taken, and how to seek further information. Notification may not be required where the data was unintelligible to unauthorised parties (e.g. strongly encrypted), where subsequent measures mean the high risk is no longer likely, or where individual notification would involve disproportionate effort (in which case a public communication is used).

Step 6 — Record and review

All breaches are recorded in the breach register (Appendix B), regardless of whether they are notified, including the facts, effects, and remedial action (Article 33(5)). After each incident a short review identifies lessons learned and any changes to controls.

5. PROCESSOR BREACHES

Processors (e.g. Marca Media, the infrastructure provider, Parademics, and event-management suppliers) are contractually required to notify Espire without undue delay on becoming aware of a breach. On receiving such a notification, Espire follows steps 2–6 above.

6. TESTING, TRAINING AND REVIEW

- All staff receive awareness of how to recognise and report a breach at induction and at least annually.
- This procedure is tested (e.g. a tabletop exercise) at least annually.
- The procedure is reviewed annually or after any significant breach or change.



DATA PROTECTION IMPACT ASSESSMENT (DPIA)

DATA PROTECTION IMPACT ASSESSMENT

1. CONTROLLER DETAILS

Name of Controller: Espire Education Group Limited

Subject/Title of DPO: Data Protection Officer

Name of Controller Contact/DPO: James Foster Le-Grys

2. THE NEED FOR A DPIA

The STEM On Track programme, operated by Espire Education, aims to deliver an educational initiative combining STEM learning with practical activities, including access to the Race Academy platform and race day events.

The programme now processes special category data (ethnicity, health) about children, and that this revision is triggered by a significant change (new sign-on, EDI, health, photos).

3. DATA COLLECTION AND PROCESSING

3.1 NATURE OF THE PROCESSING

Collection: Personal data is collected directly from schools, teachers, and students. Teacher data (names, email addresses, postal addresses, finance team contacts) is gathered via registration forms. Student data (names, email addresses) is collected for Race Academy platform access.

Use: Teacher data is used for programme administration and communication. Student data enables platform access and ensures safety/insurance compliance on race days. Data is processed to deliver educational content, manage events, and communicate updates.

Storage: Data is stored securely on Google Cloud and AWS platforms (UK/EEA-based) with encryption and restricted access to two authorised Espire Education staff.

Deletion: Teacher data is retained for the duration of participation plus 3 months; student data is retained for the academic year plus 3 months. Backups are deleted within 30 days of retention period end or upon request.

Sharing: Limited data is shared with Marca Media (UK-based) for technical troubleshooting of the Race Academy platform, our Events Management consultant and with private paramedics for race day safety/insurance. No other third-party sharing occurs without consent.

3.2. SCOPE OF THE PROCESSING

Nature of Data: Personal data includes teacher names, email addresses, postal addresses, and finance team contacts; student names, email addresses, date of birth, gender, year group, ethnicity (special category), the driver health declaration (special category), and marketing photographs.

Volume: Data is collected for all participating teachers and students (estimated 100+ schools, 100-200 teams annually, with multiple students per team).

Frequency: Data is collected at registration, updated as needed, and collected on race days.

Retention: Teacher data: duration of participation + 3 months; student data: academic year + 3 months; race day data: deleted post-event unless legally required.

Individuals Affected: Teachers and students (primarily aged 13+, with parental consent for under 13s) across participating UK schools.

Geographical Area: Data is processed and stored in the UK/EEA.

3.3 CONTEXT OF THE PROCESSING

Relationship: Data subjects are teachers (school representatives) and students participating voluntarily in an educational programme. Schools provide data on behalf of students.

Control: Individuals can exercise UK GDPR rights (e.g., access, erasure) via info@espireeducation.co.uk. Students under 13 require parental consent.

Expectations: Data use aligns with expectations for educational programme participation (platform access, event safety). No novel or unexpected processing occurs.

Vulnerable Groups: Students (including those under 13) are involved. Parental consent is required for the collection of ethnicity data for all students, regardless of background, given its status as special category data.

Technology: Google Cloud and AWS use industry-standard encryption (ISO 27001, SOC 2 compliant). No known security flaws.

Public Concerns: No specific public concerns identified; processing is standard for educational programmes.

Codes of Conduct: No approved code of conduct or certification scheme is currently adopted.

3.4 PURPOSES OF THE PROCESSING

Objectives: To deliver the STEM On Track programme, providing access to educational resources via the Race Academy platform, managing race day events, character personalisation, diversity monitoring, driver safety, marketing and communicating with schools.

Effect on Individuals: Minimal impact; data is used to facilitate participation and ensure safety. No direct marketing or communication to students occurs.

Benefits: Enhances STEM education, enables diverse student engagement, fosters practical skills, and ensures safe event participation. Benefits Espire Education by enabling programme delivery and compliance.

4. CONSULTATION PROCESS

Stakeholders: Schools and teachers will be consulted during programme onboarding to ensure data processing is understood. Parental consent obtained via Race Academy for students under 13 and for all special category data and marketing purposes.

Internal Involvement: The DPO (or equivalent contact) and two authorised staff managing the Race Academy platform will review data processes.

Processors: Marca Media will be consulted for technical compliance with AWS. Paramedics will confirm race day data handling protocols.

Experts: Information security experts (consulted via Google Cloud/AWS documentation) ensure platform security. No external security consultants are currently engaged.

Justification for Non-Consultation: Student consultation is not feasible due to age and scale; schools act as intermediaries. Parental consent ensures under-13s' interests are represented.

5. NECESSITY AND PROPORTIONALITY

Lawful Basis:

- **Consent:** For marketing (e.g., newsletters, photographs), explicit consent is obtained from the parent/guardian, withdrawable at any time via info@espireeducation.co.uk.
- **Legitimate Interest:** For essential programme administration, including platform access, school communication, and management of necessary participation data (name, school email, date of birth).
- **Legal Obligation:** For race day insurance/safety compliance.
- **Explicit Consent (Art. 9(2)(a)):** For special category data — ethnicity (used for character personalisation) and the driver medical/fitness declaration — explicit parental consent is obtained, in addition to the Article 6 basis above. Special category data requires both an Article 6 lawful basis and an Article 9 condition; legitimate interest alone is not sufficient. In a genuine medical emergency, we may also rely on the vital interests condition (Article 9(2)(c)) to share the driver medical declaration with on-site medical providers if it is not possible to confirm consent at that moment.
- **Equality Condition (DPA 2018, Sch. 1, Pt. 2, para. 8):** For aggregate EDI/diversity monitoring, processing also relies on the equality-of-opportunity condition. Reliance on this condition requires an Appropriate Policy Document to be maintained, covering compliance with the data-protection principles and our retention and erasure approach for this data.

Necessity: Processing is essential for delivering the programme, managing events, and ensuring safety. No alternative method achieves these outcomes without personal data.

Necessity: Processing is essential for delivering the programme, managing events, and ensuring safety. No alternative method achieves these outcomes without personal data.

Function Creep Prevention: Data is used only for specified purposes (platform access, event management, communication, character personalisation, EDI monitoring, driver safety, marketing). Regular reviews ensure adherence.

Data Quality/Minimisation: Only necessary data is collected. Date of birth, rather than age alone, is collected because it is necessary to apply the age-13 consent threshold accurately and to verify driver eligibility against a fixed date (drivers must be 16 or under by 1 June 2027). Optional and special category data (EDI, the driver declaration, photographs) is collected only where the corresponding parental consent has been recorded, enforced through the platform design rather than relying on supervision. Regular checks ensure accuracy.

Information to Individuals: The Race Academy Privacy Policy is shown to parents at the point consent is sought, and schools are informed of data use during registration. Individuals can access rights via info@espireeducation.co.uk.

Supporting Rights: Requests for access, rectification, or erasure are handled promptly via email. Processes are in place to verify and action requests.

Processor Compliance: Contracts with Marca Media include UK GDPR-compliant terms. Regular audits ensure adherence.

International Transfers: No transfers outside UK/EEA; data is hosted in UK/EEA-based servers.

DPIA RISK REGISTER

R I S K R A T I N G S					
Risk	Source of Risk	Potential Impact	Likelihood of Harm	Severity of Harm	Overall Risk
1	Unauthorised access to Google Cloud/AWS	Data breach exposing teacher/student data	Remote	Significant	Medium
2	Data retention beyond necessary period	Privacy violation, non-compliance with UK GDPR	Possible	Minimal	Low
3	Lack of parental consent for under-13s	Non-compliance with UK GDPR, potential harm to children	Possible	Significant	Medium
4	Third-party misuse	Unauthorised data use or retention	Remote	Significant	Medium
5	Inaccurate data affecting platform access	Disruption to programme participation	Possible	Minimal	Low
6	Obtaining and Processing Children’s Special Category Data	Consent not technically enforced, re-identification from small cohorts, health-data retention, and marketing images after withdrawal.	Possible	Significant	High

MEASURES TO REDUCE RISK

Risk	Options to Reduce or Eliminate Risk	Effect on Risk	Residual Risk	Measure Approved
1	Use of ISO 27001/SOC 2-compliant Google Cloud/AWS with encryption and restricted access (two staff only).	Reduced	Low	Yes
2	Defined retention periods (academic year + 3 months for students; participation + 3 months for teachers); automated deletion and 30-day backup removal	Eliminated	Low	Yes
3	Parental consent obtained via schools for under-13s; age verification during registration	Eliminated	Low	Yes
4	Contracts with Marca Media include UK GDPR clauses; limited access and no data retention by third parties	Reduced	Low	Yes <i>*Contract to be reviewed in next quarterly meeting</i>
5	Regular data accuracy checks during registration; schools prompted to update teacher/student details annually	Eliminated	Low	Yes
6	System gating, prefer-not-to-say option, aggregation with small-cell suppression, withdrawable photo consent, and the Appropriate Policy Document.	Reduced	Low	Yes

SIGN OFF & RECORDED OUTCOMES

Item	Position	Name	Date Signed-off	Notes
Measures Approved By	Director	Adam Sirett	Jun 16, 20...	Integrate actions into project plan by 01/12/25, assigned to Ipek Taskin (Programme Co-ordinator)
Residual Risks Approved By	Director	Adam Sirett	Jun 16, 20...	All residual risks are low; no ICO consultation required.
DPO Advice Provided	Director	James Foster Le-Grys	Jun 17, 20...	DPO confirmed compliance with UK GDPR, adequacy of measures, and processing approval.
Summary of acting DPO Advice	Director	James Foster Le-Grys	Jun 17, 20...	The acting DPO, James Foster Le-Grys, has reviewed the processing covered by this DPIA, including EDI data, the driver medical/fitness declaration, marketing photographs, and the parent-routed consent process. Security, retention, and consent arrangements are appropriate; ethnicity and the driver declaration are correctly treated as special category data under explicit consent, supported by the equality condition and Appropriate Policy Document for aggregate EDI monitoring, with vital interests available for emergency paramedic disclosure. The driver declaration's retention of full medical detail until the National Finals is a higher residual risk than previously envisaged (see Risk 6), and processor due diligence should extend to the paramedic provider. The processing aligns with Section 5's lawful bases; the storage provider and Greater China items remain outstanding and should be confirmed. Two short paragraphs. The three load-bearing points are still there — special category treatment, the named risk increase with its register cross-reference, and the open items — just carried in fewer words.
DPO Advice Accepted/Overruled By	Director	Adam Sirett	Jun 24, 20...	Accepted.
Consultation Responses Reviewed By	Director	Adam Sirett	Jun 24, 20...	School and parental feedback will be reviewed; deviations from views will be justified.
DPIA Kept Under Review By	Director	James Foster Le-Grys	Jun 24, 20...	Annual review scheduled for July 20th 2026 or upon significant programme changes.

READY TO RACE

At STEM On Track, operated by Espire Education, we are steadfast in our commitment to protecting your personal data and ensuring compliance with the UK Data Protection Act 2018 and UK GDPR. We strive to process your information transparently, securely, and only as necessary to deliver our educational programme. Should you have any questions, wish to exercise your data protection rights, or seek further information about our practices, please contact us at:

 info@espireeducation.co.uk

We value your trust and are dedicated to maintaining the highest standards of data protection in all our activities.

APPENDIX

APPENDIX A

INTERNAL BREACH REPORT

Reported by / role	
Date and time of discovery	
Date and time of the incident (if known)	
What happened (description)	
Data and individuals affected (incl. any children / special category)	
Estimated number of individuals / records	
Immediate containment steps taken	
Has any third party / processor been involved?	
Any other information	

APPENDIX B

BREACH LOG

This document serves as the official Personal Data Breach Log for Espire Education, maintained in accordance with Article 33(5) of the UK/EU GDPR to record the facts, effects, and remedial actions taken for all identified data security incidents.

Ref	Date Aware	Summary	ICO Notified?	Individuals Notified
			Y/N	Y/N
			Y/N	Y/N
			Y/N	Y/N
			Y/N	Y/N
			Y/N	Y/N