NEW AVENUE
SCHOOL

Policy Name	Data Protection Policy
Policy No.	NA10
Date Written	12.01.24
Date to Review	03.09.26
Author	Anthony Merriman
Cross Reference	• Safeguarding and Child Protection Policy • ICT and Acceptable Use Policy • Risk Assessment Policy • Attendance and Admissions Policy • Complaints Policy

1. Aims

New Avenue School collects, uses, stores, and shares personal data about pupils, parents/carers, staff, and third parties. This policy sets out how we meet our duties under the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and the **Data Protection and Digital Information Act 2025 (DUAA 2025)**.

The aims of this policy are to:

- Protect the rights and freedoms of individuals whose personal data we process.
- Demonstrate accountability and transparency in line with statutory expectations, including the **Independent School Standards (ISS 2025)**.
- Safeguard pupils by ensuring that all processing of personal data supports the principles in **Keeping Children Safe in Education (KCSIE 2025)**, including online safety, filtering/monitoring, and safeguarding records.
- Provide clear responsibilities for staff, governors, and contractors in handling personal data securely and lawfully.
- Embed data protection into our SEMH focused provision, recognising that safeguarding, attendance, and therapeutic records form part of pupils’ data profiles.
- Ensure that personal data is used to support education, safeguarding, and welfare, and never processed in ways that could cause harm.

- Provide a framework for handling Subject Access Requests (SARs), breaches, and complaints in line with ICO and DfE guidance.

2. Legislation and Guidance

This policy is based on the following legislation, statutory frameworks, and guidance:

Core Data Protection Legislation

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data Protection and Digital Information Act 2025 (DUAA 2025) – clarifies data rights, introduces recognised legitimate interests (including safeguarding), and updates handling of Subject Access Requests and records of processing.

Education and Safeguarding Duties

- Keeping Children Safe in Education (KCSIE 2025) – expectations around processing and sharing safeguarding data, online safety monitoring, and data transfer between schools.
- Working Together to Safeguard Children (2023) – duties to share information across agencies to protect children.
- Independent School Standards (ISS 2025), Part 3 – requirement to protect pupils' welfare, which includes lawful management of their personal data.
- Education (Pupil Registration) Regulations 2006 (as amended 2024) – expectations on record-keeping and data transfer for admissions and leavers.
- SEND Code of Practice (2015) – requirements on storing and sharing information to support EHCPs and statutory reviews.

Specific Areas of Risk

- DfE Filtering and Monitoring Standards (2025) – requirement to risk assess and document the processing of filtering and monitoring logs.
- ICO guidance on Data Sharing and Safeguarding – expectations on lawful sharing of safeguarding information without consent where necessary.
- Information and Records Management Society (IRMS) Schools Toolkit (2024 edition) – recommended retention and disposal schedules for education records.
- Human Rights Act 1998 and Equality Act 2010 – duties to protect individual rights when processing data.

3. Definitions

Personal data

Any information that relates to an identified or identifiable individual. This includes basic details (name, address, date of birth) as well as information about safeguarding, behaviour, attendance, health, or online activity.

Special category data

Sensitive personal data requiring additional protection under UK GDPR and the Data Protection Act 2018, such as:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Health information (including mental health, SEMH, anxiety, EBSA-related data)
- Genetic and biometric data
- Sexual orientation

Processing

Any operation performed on personal data, whether automated or manual, including collection, storage, retrieval, sharing, analysing, or deletion.

Data subject

The identified or identifiable person whose personal data is being processed. At New Avenue School, this includes pupils, parents/carers, staff, contractors, and visitors.

Data controller
The organisation responsible for deciding how and why personal data is processed. New Avenue School is the data controller for the personal data we hold.

Data processor
An organisation or person (other than an employee of the controller) that processes data on behalf of the controller, such as Oakford Technology (ICT support) or online learning platforms.

Data Protection Officer (DPO)
The named person responsible for overseeing data protection strategy and compliance.

Safeguarding data
Records linked to safeguarding, behaviour, attendance, EBSA interventions, risk assessments, and child protection files. This data is processed under safeguarding obligations as a recognised legitimate interest under DUAA 2025.

Filtering and monitoring data
Logs and reports generated by ICT systems that track access to online content, attempts to bypass filters, or alerts of potential safeguarding concerns. These are classed as personal data and are mapped in the school's Record of Processing Activity (RoPA).

AI-generated data
Data created by AI tools (e.g. text, images, analysis reports) used in teaching, administration, or monitoring. Where this data relates to identifiable individuals, it is treated as personal data under UK GDPR/DUAA 2025.

Subject Access Request (SAR)
A request by a data subject (or parent/carer on their behalf, depending on age and capacity) to access personal data held by the school. Under **DUAA 2025**, schools may refuse or charge for repetitive or manifestly unfounded SARs, but safeguarding data remains accessible where it is in the child's best interests.

4. Data Protection Principles

New Avenue School processes personal data in line with the principles set out in the **UK GDPR, Data Protection Act 2018, and DUAA 2025**.

We ensure that personal data is:

1. **Lawfulness, fairness and transparency** – processed lawfully, fairly and in a transparent manner.
    - Parents, pupils, and staff are informed via privacy notices about how their data is used.
    - Safeguarding data is processed under legitimate interests recognised in DUAA 2025, without requiring consent where this protects a child from harm.
2. **Purpose limitation** – collected for specified, explicit and legitimate purposes.
    - Examples include: delivering education, safeguarding, EBSA interventions, monitoring attendance, complying with ISS 2025, and meeting legal obligations.
3. **Data minimisation** – adequate, relevant, and limited to what is necessary.
    - The school will not collect or retain excessive data, and will review forms and systems annually.
4. **Accuracy** – accurate and, where necessary, kept up to date.
    - Parents and staff are asked to update contact and medical details promptly.
    - Safeguarding records are checked regularly for accuracy by the DSL.
5. **Storage limitation** – kept for no longer than necessary.
    - Data is retained in line with the IRMS Schools Toolkit 2024 and statutory retention schedules.
    - Safeguarding and EBSA-related records are stored until the pupil reaches 25 years old, unless legal advice states otherwise.
6. **Integrity and confidentiality (security)** – processed securely using appropriate technical and organisational measures.
    - Systems use encryption, MFA, and access restrictions.
    - Filtering/monitoring data is accessible only to the DSL, Headteacher, and ICT Lead.

7. **Accountability –** the school is responsible for, and must be able to demonstrate, compliance with all principles.
   - The school maintains a Record of Processing Activity (RoPA).
   - Data Protection Impact Assessments (DPIAs) are carried out for high-risk processing, including new safeguarding systems, filtering/monitoring, or AI tools.

5. Roles and Responsibilities

Governing Board

The governing board has strategic responsibility for ensuring New Avenue School complies with all data protection legislation. Governors will:

- Scrutinise compliance with UK GDPR, Data Protection Act 2018, and DUAA 2025.
- Receive termly reports on data protection, safeguarding data processing, and filtering/monitoring outcomes.
- Ensure the Record of Processing Activity (RoPA) is maintained and reviewed annually.
- Approve this policy and oversee its implementation.

Headteacher

As the school's **Data Controller**, the Headteacher is responsible for:

- Implementing this policy and embedding data protection into daily school operations.
- Ensuring data protection is considered in all new projects, systems, and safeguarding arrangements.
- Ensuring staff are trained in data protection, cyber security, and safeguarding data handling.
- Reporting significant data breaches to the governors and, with the DPO, to the ICO where required.

Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Ensuring safeguarding and EBSA-related data (child protection files, risk assessments, attendance records, filtering/monitoring alerts) is processed lawfully and securely.
- Overseeing secure transfer of safeguarding files within statutory timeframes (KCSIE 2025).
- Working with the DPO to ensure lawful data sharing with external agencies in line with Working Together 2023.
- Advising staff on lawful sharing of information without consent where a child is at risk of harm, under DUAA 2025 recognised legitimate interests.

Data Protection Officer (DPO)

The DPO is responsible for:

- Advising on compliance with UK GDPR and DUAA 2025.
- Monitoring and auditing practice across the school.
- Maintaining the Record of Processing Activity (RoPA).
- Supporting Data Protection Impact Assessments (DPIAs), especially for high-risk processing (e.g. filtering/monitoring, AI tools, new safeguarding systems).
- Acting as the point of contact with the ICO.

ICT Lead / Oakford Technology

The ICT Lead, supported by Oakford Technology, is responsible for:

- Maintaining technical security measures (encryption, MFA, access controls, secure storage).
- Managing filtering and monitoring systems, and ensuring alerts are acted upon by the DSL.
- Reporting cyber security and data risks to SLT and governors.
- Ensuring third-party processors meet contractual and legal obligations.

Staff and Volunteers

All staff and volunteers must:

- Follow this policy and all training provided.
- Handle personal and safeguarding data securely, including EBSA-sensitive information.
- Report data breaches immediately to the Headteacher or DPO.
- Only access systems and data for which they are authorised.

Pupils and Parents/Carers

- Pupils and parents/carers have the right to request access to personal data through Subject Access Requests (SARs).
- Pupils aged 12 and above are generally considered competent to make their own SARs unless evidence suggests otherwise.
- Parents/carers must respect confidentiality of other children and staff when receiving data under a SAR.

6. Collecting Personal Data

6.1 Lawful Basis

New Avenue School collects personal data only where there is a clear lawful basis under **UK GDPR, the Data Protection Act 2018, and DUAA 2025**. These include:

- **Legal obligation** – meeting duties under education, safeguarding, and employment law.
- **Public task** – delivering education and safeguarding in the public interest.
- **Contract** – where processing is necessary for a contract with staff or third parties.
- **Consent** – used only for optional activities (e.g. marketing, photography, off-site enrichment not part of statutory provision).
- **Legitimate interests (DUAA 2025 recognised categories)** – safeguarding, preventing crime, ensuring network and information security.

6.2 Types of Data Collected

We collect and process data including:

- **Pupils** – personal details, EHCPs, attendance and behaviour records, safeguarding and EBSA information, assessment data, health/medical details, filtering and monitoring logs.
- **Parents/carers** – contact information, safeguarding details, consents, correspondence.
- **Staff** – employment records, payroll data, training, safeguarding information, performance data.
- **Contractors/visitors** – identification and safeguarding checks.

6.3 Safeguarding and EBSA-Specific Data

We also collect information necessary to meet our SEMH and EBSA-specialist provision:

- Risk assessments linked to anxiety, EBSA, or behaviour.
- Therapeutic records and attendance reintegration plans.
- Safeguarding logs and multi-agency reports.
- Filtering/monitoring alerts that indicate safeguarding risks.

6.4 Fair Processing

- Individuals are informed of how their data will be used through **Privacy Notices**, published on the school website and available in paper form.
- Pupils and parents/carers are informed in clear, accessible language, with EBSA-sensitive adjustments (e.g. phased sharing during reintegration).
- Personal data is collected directly from the individual wherever possible. When collected from third parties (e.g. previous schools, social care, health providers), this is done securely and lawfully.

6.5 Accuracy and Updates

- Parents/carers and staff are expected to notify the school of changes to contact or medical details.
- Attendance, safeguarding, and EBSA records are checked regularly by the DSL and SLT to ensure accuracy.
- Inaccuracies are corrected without delay.

7. Sharing Personal Data

7.1 Statutory and Safeguarding Duties

We share personal data where required by law, or where it is necessary to protect the welfare of a child. This includes:

- **Safeguarding and child protection concerns** – shared without consent where there is risk of harm, in line with **KCSIE 2025** and **Working Together 2023**.

- **Attendance and EBSA records –** shared with Local Authorities where pupils are persistently absent, in line with statutory duties.
- **Admissions and leavers –** pupil records transferred within statutory timescales under the **Education (Pupil Registration) Regulations 2006, as amended 2024**.

7.2 External Agencies and Partners

We share data with trusted partners where it supports education, welfare, and safeguarding, including:

- Local Authorities and Virtual Schools
- Health and therapeutic services (e.g. CAMHS, SALT, OT)
- Social care and multi-agency safeguarding partners
- The Department for Education (DfE) and Ofsted
- Examination boards
- Police and other emergency services
- Technology providers who support education and safeguarding (e.g. Oakford Technology, filtering and monitoring providers)

7.3 Filtering and Monitoring Data

- Logs and alerts generated by filtering/monitoring systems are treated as personal data.
- These may be shared with the DSL, SLT, governors, and external safeguarding agencies where risks are identified.
- Such sharing is lawful under **DUAA 2025 recognised legitimate interests** (safeguarding and security).

7.4 Consent and Optional Sharing

- Where consent is required (e.g. school photographs, optional enrichment activities, marketing), this will be sought in writing.
- Consent can be withdrawn at any time by contacting the school.

7.5 Secure Transfer

- All data transfers are carried out securely using encrypted email, secure portals, or recorded delivery.
- The DSL confirms receipt of safeguarding records when pupils join or leave the school.
- Where records are not received, the DSL escalates with the previous/receiving setting and Local Authority.

7.6 International Transfers

- Personal data will not be routinely transferred outside the UK.
- Where international transfers are unavoidable (e.g. cloud-based systems), the school will ensure adequate safeguards in line with UK GDPR and **DUAA 2025**.

8. Subject Access Requests and Other Rights of Individuals

8.1 Rights of Individuals

Under **UK GDPR**, the Data Protection Act 2018, and the **Data Protection and Digital Information Act 2025 (DUAA 2025)**, individuals have the right to:

- Access personal data held about them (Subject Access Request).
- Request rectification of inaccurate or incomplete data.
- Request erasure of data (the "right to be forgotten") where there is no legal basis to retain it.
- Restrict processing in certain circumstances.
- Object to processing carried out under legitimate interests or public task.
- Request data portability (where applicable).
- Challenge automated decision-making or profiling (including AI tools).

These rights are subject to exemptions where data must be retained for safeguarding, legal, or public interest reasons.

8.2 Subject Access Requests (SARs)

- SARs can be made verbally or in writing to any member of staff, but must be passed immediately to the **DPO**.
- Requests will be processed within **one month**, unless they are complex, in which case the deadline may be extended by up to two months.

- **DUAA 2025** allows schools to:
  - Refuse manifestly unfounded or excessive SARs.
  - Charge a reasonable fee for repetitive requests.
- Safeguarding records may be withheld or redacted where release would put a child at risk.

8.3 SARs from Pupils and Parents/Carers

- Pupils aged **12 and above** are generally considered competent to request access to their own data, unless evidence suggests otherwise.
- Parents/carers can make SARs on behalf of their child where the child is not competent or where it is in the child's best interests.
- The **DSL and DPO** will advise on SARs involving safeguarding records to balance transparency with the protection of the child.

8.4 Responding to SARs

The school will:

- Verify the identity of the requester.
- Provide the data in a secure, accessible format.
- Redact information relating to other individuals unless consent is obtained.
- Keep a log of all SARs, responses, and decisions for accountability.

9. Parental Requests to see Educational Records

9.1 Right of Access

- Parents/carers have the right to request access to their child's educational record.
- An educational record includes information about the pupil that is processed for the purpose of education, training, or welfare.
- Requests may be made verbally or in writing and must be passed immediately to the Headteacher or DPO.

9.2 Scope and Exemptions

- Access will normally be granted unless:
  - Information relates to another individual and cannot reasonably be redacted.
  - Release would cause serious harm to the physical or mental health of the pupil or another person.
  - Safeguarding records are involved and disclosure would put a child at risk of harm.
- The DSL and DPO will review all safeguarding-related requests before release.

9.3 Timeframe and Fees

- Requests will be fulfilled within **15 school days** in line with education regulations.
- Under **DUAA 2025**, the school may:
  - Refuse requests that are manifestly unfounded or excessive.
  - Charge a reasonable fee for repetitive requests.

9.4 Format of Response

- Records will be provided in a secure format (encrypted electronic file or paper copy by recorded delivery).
- A covering explanation will be provided to help parents/carers understand the contents.
- Where information is withheld, the reasons will be explained in writing.

10. Photographs and Videos

10.1 Lawful Use

- The school uses photographs and videos of pupils for educational, welfare, and promotional purposes.
- Such processing is carried out on the basis of **consent** or **legitimate interests**, depending on the context:
  - **Consent** – for external use (e.g. website, social media, newsletters, marketing).
  - **Legitimate interest** – for internal use (e.g. classroom displays, progress tracking, safeguarding records).

10.2 Safeguarding and EBSA Considerations

- Staff must always consider safeguarding implications before capturing or sharing images.
- Photographs or videos must **never be taken if they could place a pupil at risk**, particularly those subject to safeguarding restrictions, high-anxiety presentations, or EBSA support plans.
- The **DSL maintains a list of pupils with restricted image permissions**, and staff must check this before capturing or publishing images.
- Photography and video are prohibited in **sensitive contexts** (e.g. toilets, changing rooms, medical support areas).

10.3 Consent Management

- Consent for photography/video use is sought from parents/carers on admission and reviewed annually.
- Pupils' views are also taken into account, particularly where anxiety or EBSA-related concerns exist.
- Consent can be withdrawn at any time by notifying the school in writing.

10.4 Secure Storage and Use

- Images and videos are stored securely on the school's network or authorised platforms, with access limited to staff who need it.
- Staff must not use personal devices for capturing or storing images of pupils.
- Any external photographers (e.g. school photography companies) must be approved, supervised, and comply with data protection law.

10.5 Sharing and Publication

- Images for external use will only be shared in line with recorded parental consent.
- Pupils will not be identified by full name alongside photographs in external publications unless parental consent is explicitly given.
- The school will never share images in ways that enable **location tracking** or could increase safeguarding risks.

11. Artificial Intelligence (AI)

11.1 Use of AI in School

- AI tools may be used to support teaching, administration, or safeguarding functions, such as:
  - Lesson planning or resource creation.
  - Data analysis for attendance or assessment.
  - Filtering and monitoring alerts.
- All AI use must be **lawful, proportionate, and transparent**, and comply with the principles in **UK GDPR, the Data Protection Act 2018, and DUAA 2025**.

11.2 Risks and Safeguards

- AI-generated outputs that contain or relate to identifiable individuals are treated as **personal data**.
- Staff must not input sensitive personal data (e.g. safeguarding, EBSA, medical, or HR data) into external AI tools unless explicitly authorised and subject to a DPIA.
- The school will conduct **Data Protection Impact Assessments (DPIAs)** before adopting new AI systems, particularly where processing could affect safeguarding or pupil welfare.
- AI will not be used for automated decision-making that has a significant impact on individuals without human oversight.

11.3 Safeguarding and EBSA

- AI systems used for filtering/monitoring are overseen by the **DSL and ICT Lead**, who assess alerts in line with safeguarding duties under **KCSIE 2025**.
- The school recognises that AI systems may misinterpret EBSA or anxiety-related behaviours. Staff must apply professional judgment and avoid over-reliance on automated outputs.
- AI will not be used in ways that could stigmatise or profile pupils with SEMH or EBSA needs.

11.4 Accountability

- The **Headteacher and DPO** are responsible for ensuring AI use complies with data protection law.
- The **DPO** maintains the Record of Processing Activity (RoPA), including any AI-related processing.

- The school will keep an **AI Register**, recording tools in use, their purpose, and the outcomes of DPIAs.

11.5 Training

- Staff will receive training on:
  - Appropriate use of AI tools in education.
  - Risks of bias, inaccuracy, or safeguarding gaps.
  - Data protection and DUAA 2025 requirements for AI.
- Pupils will be educated about the safe and responsible use of AI as part of the curriculum, linked to online safety and critical thinking.

12. Data Protection and Design by Default

12.1 Embedding Data Protection

- The school applies the principle of **"data protection by design and by default"** in all systems, projects, and practices.
- This means that privacy and data protection are considered from the outset and are built into decision-making, not added afterwards.
- Only the **minimum necessary personal data** is collected, processed, and retained for each purpose.

12.2 Safeguarding and EBSA

- Systems are designed to protect the confidentiality and security of **safeguarding and EBSA-related data**, recognising the sensitivity of these records.
- Access to such data is **strictly role-based**, with logs of who has accessed safeguarding information.
- Filtering/monitoring systems are configured to flag concerns to the DSL while minimising unnecessary intrusion.

12.3 Technical and Organisational Measures

- New systems and processes are subject to a **Data Protection Impact Assessment (DPIA)**, especially where they involve:
  - Safeguarding or health data.
  - EBSA or attendance records.
  - Filtering/monitoring logs.
  - AI tools or automated processing.
- Encryption, multi-factor authentication (MFA), secure storage, and access controls are applied by default.
- Staff accounts are restricted to the minimum data necessary to perform their role.

12.4 Accountability

- The **DPO** maintains oversight of DPIAs and ensures compliance with DUAA 2025.
- The **Headteacher and governors** monitor that design-by-default principles are embedded in procurement, system use, and daily practice.
- Suppliers and contractors must demonstrate compliance with data protection law before systems or services are adopted.

13. Data Security and Storage of Records

13.1 Security Measures

The school takes appropriate technical and organisational steps to keep personal data secure, proportionate to the sensitivity of the data. Measures include:

- Encryption of devices and portable media.
- Secure password policies and multi-factor authentication (MFA).
- Access restricted on a **role-based basis**, ensuring safeguarding and EBSA records are available only to authorised staff.
- Filtering and monitoring logs accessible only to the **DSL, Headteacher, and ICT Lead**.
- Regular testing of firewalls, anti-virus, and endpoint protection.
- Secure backup systems, with off-site/cloud backups tested regularly for recovery.

13.2 Storage of Records

- Pupil records, including safeguarding and EBSA documentation, are kept in secure, access-controlled systems.
- Physical records (where still required) are stored in locked cabinets in restricted areas.
- Digital files are stored on the school's secure server or approved cloud services, never on personal devices.
- Sensitive records (e.g. safeguarding, therapy notes, EBSA attendance plans) are marked and stored separately with restricted access.

13.3 Retention

- Records are retained in line with statutory requirements and the **IRMS Schools Toolkit 2024**.
- Safeguarding and child protection files are retained until the pupil reaches **25 years old**, unless legal advice requires longer.
- EBSA, therapeutic, and attendance reintegration records are retained as part of the safeguarding file.
- Staff, governor, and contractor records are retained in accordance with employment and company law.

13.4 Secure Disposal

- Paper records are shredded on site or disposed of by an accredited contractor.
- Digital files are securely deleted using appropriate wiping software when retention periods expire.
- The school records all disposals in a **data destruction log**.

13.5 Accountability

- The **Headteacher and DPO** are jointly responsible for ensuring that storage and security arrangements are compliant with **DUAA 2025**.
- Governors review security arrangements annually, including outcomes from any penetration testing or cyber-security audits.

14. Disposal of Records

14.1 Principles

- Records are disposed of securely and in line with statutory requirements, the **IRMS Schools Toolkit (2024)**, and the principles of **DUAA 2025**.
- Disposal applies to both physical and digital records once retention periods have expired or data is no longer required.
- The school ensures that disposal methods protect confidentiality and prevent unauthorised access.

14.2 Physical Records

- Paper records containing personal data (e.g. pupil files, safeguarding logs, EBSA support plans) are shredded on-site or collected by an accredited confidential waste contractor.
- Contractors provide certificates of destruction, which are retained by the school for audit purposes.

14.3 Digital Records

- Digital files are securely deleted using approved deletion or wiping software, ensuring that data cannot be recovered.
- Portable devices and storage media are wiped and, if appropriate, physically destroyed before disposal.
- Cloud-based systems are checked to confirm records have been fully and permanently deleted.

14.4 Documentation and Accountability

- A **Data Destruction Log** is maintained, recording:
  - The type of record destroyed.
  - The date of destruction.
  - The staff member or contractor responsible.
- The **Headteacher and DPO** review the destruction log annually and report outcomes to governors.

14.5 Safeguarding and EBSA Records

- Extra care is taken when disposing of **safeguarding and EBSA-related records**.

- Disposal is overseen by the DSL and recorded in the safeguarding file audit trail.
- No safeguarding data is destroyed without cross-checking retention requirements with statutory guidance.

15. Personal Data Breaches

15.1 Definition

A personal data breach is any incident that results in the accidental or unlawful:

- Destruction, loss, or alteration of personal data.
- Unauthorised disclosure of, or access to, personal data.
- Failure to protect safeguarding, EBSA, or filtering/monitoring data in a way that risks the rights and freedoms of individuals.

15.2 Reporting by Staff

- All staff, contractors, and volunteers must **immediately report suspected or actual breaches** to the Headteacher and DPO.
- Where safeguarding data is involved, the **DSL must also be informed at once**.
- Staff should not attempt to investigate or resolve breaches themselves.

15.3 Investigation

The Headteacher and DPO will:

- Record the breach in the **Data Breach Log**.
- Investigate to establish the scope, cause, and risk to individuals.
- Work with the DSL if safeguarding data or EBSA information is involved.
- Decide whether the breach is notifiable to the ICO, DfE, or affected individuals.

15.4 Notification

- The **ICO** will be notified within **72 hours** of discovery where the breach is likely to result in a risk to individuals' rights and freedoms.
- Affected individuals will be informed promptly, in clear and accessible language, if the breach is likely to result in a high risk to them.
- Where safeguarding or EBSA data is involved, the DSL will coordinate with **social care and safeguarding partners** as appropriate.
- The **DfE** may also be notified if the breach impacts education delivery or pupil welfare.

15.5 Preventive Measures

Following a breach, the school will:

- Take immediate steps to contain and mitigate harm.
- Review policies, procedures, and technical systems.
- Deliver refresher training to staff where appropriate.
- Update Data Protection Impact Assessments (DPIAs) if new risks are identified.
- Report lessons learned to governors for oversight.

16. Training

16.1 Staff Training

- All staff, volunteers, governors, and contractors with access to personal data receive training on data protection at induction and **refresher training annually**.
- Training covers:
  - Principles of **UK GDPR, the Data Protection Act 2018, and DUAA 2025**.
  - Handling and securing **safeguarding and EBSA records**.
  - Lawful information-sharing under **KCSIE 2025** and **Working Together 2023**.
  - Responding to Subject Access Requests (SARs).
  - Recognising and reporting data breaches.
  - Secure use of ICT systems, including filtering and monitoring logs.
  - Appropriate and lawful use of **AI tools**.

16.2 Safeguarding Emphasis

- Staff are trained to understand that **safeguarding data is personal data** and must be processed lawfully and securely.
- Special focus is given to handling sensitive **EBSA-related information**, where disclosure could impact pupil welfare or attendance.
- The DSL provides targeted updates where safeguarding guidance changes (e.g. **KCSIE annual updates**).

16.3 Specialist Training

- The **DPO** receives advanced training to remain up to date with data protection law, ICO guidance, and DUAA 2025 provisions.
- The **ICT Lead and Oakford Technology** receive specialist training on cyber security, filtering/monitoring, and secure data storage.
- Governors receive annual training to support their oversight role.

16.4 Ongoing Awareness

- Data protection reminders are built into staff meetings, supervision sessions, and safeguarding briefings.
- Staff are updated immediately on changes to law, regulation, or local safeguarding procedures.
- Scenarios and case studies are used to reinforce learning and apply principles to real school contexts.

17. Protection of Children's Biometric Information

17.1 Definition

Biometric data is personal information obtained from pupils that uses their physical or behavioural characteristics for identification, such as:

- Fingerprints
- Facial recognition
- Voice patterns
- Iris or retina scans

Under the **Data Protection Act 2018**, **UK GDPR**, and **DUAA 2025**, biometric data is classed as **special category data** and must be processed with extra care.

17.2 Legal Duties

The school will comply with the **Protection of Freedoms Act 2012** by ensuring that:

- No child's biometric information is processed without the **written consent of at least one parent/carer**.
- If one parent/carer objects, the biometric data will not be taken or used, even if the other consents.
- Pupils themselves may object to the processing of their biometric data at any time, and their objection will override parental consent.

17.3 Safeguarding and EBSA Considerations

- The school recognises that pupils with **high anxiety or EBSA** may find biometric systems distressing.
- Alternative identification methods (e.g. ID cards, PIN codes) will always be available and explained clearly to pupils and parents.
- No pupil will be disadvantaged or stigmatised for refusing to participate in biometric systems.

17.4 Transparency and Fair Processing

- Parents/carers and pupils will be provided with clear information about:
  - What biometric data will be used for.
  - How it will be stored securely.
  - How long it will be retained.
  - Who will have access to it.
- Biometric data will never be shared with third parties except where required by law.

17.5 Security and Disposal

- Biometric data will be stored securely, with encryption and access controls.
- Data will be deleted when the pupil leaves the school, or earlier if consent is withdrawn.

- Disposal will be recorded in the **Data Destruction Log**.

18. Monitoring and Evaluation

18.1 Oversight

- The **Headteacher** has overall responsibility for implementing this policy.
- The **DPO** monitors compliance with data protection law, audits practice, and advises on improvements.
- The **DSL** oversees the processing of safeguarding and EBSA-related data to ensure compliance with **KCSIE 2025**.
- The **governing board** provides strategic oversight, receiving termly reports on:
    - Data protection compliance.
    - Data breaches and lessons learned.
    - Filtering and monitoring outcomes.
    - Safeguarding and EBSA-related data processing.

18.2 Review Cycle

- This policy is reviewed **annually**, or sooner if:
    - There are changes to data protection law (e.g. updates to **DUAA 2025**).
    - Statutory safeguarding guidance is updated (e.g. **KCSIE annual revisions**).
    - New technologies are introduced that impact data processing (e.g. AI systems, new safeguarding platforms).
    - A significant data breach or safeguarding incident identifies gaps in practice.

18.3 Continuous Improvement

- Findings from audits, incident reviews, and ICO or DfE feedback are built into future policy updates.
- Training and staff awareness sessions are updated regularly to reflect new risks or legal requirements.
- The school is committed to a culture of **accountability and transparency**, ensuring that personal data is processed lawfully, fairly, and in the best interests of pupils.

Updates

Dates	Comments
07.03.25	Updated for UK GDPR compliance requirements, including DPIAs, SARs, retention, and breach reporting in line with ICO and DfE guidance.
16.09.25	Full review following enactment of the Data Protection and Digital Information Act 2025 (DUAA 2025). Policy updated to: reference DUAA throughout; align with KCSIE 2025 and ISS 2025; embed processing of safeguarding, EBSA, and filtering/monitoring data into RoPA; strengthen SAR handling (including age 12+ competence and DUAA provisions on unfounded/excessive requests); add sections on AI use and design-by-default; update retention and disposal in line with IRMS 2024 Toolkit; clarify DSL/DPO oversight for safeguarding data; expand breach management and governor oversight.