Engaging Eyes Ltd

Data Protection Policy

APPROVED: **Nov 2020**

REVIEW: **Nov 2023**

Date of next review: July 2025

Contents

Issue Status

Date	Issue	Date Approved	Review date
26.11.2020	v.1 draft policy written by Global Policing.		
28.11.2021	V.2 addition added to video recording section		
13.11.2023	V.3 updated by Alex Old		

1. Aims

Our Company aims to ensure that all personal data collected about staff, service users, visitors and other individuals is collected, stored and processed in accordance with the The UK General Data Protection Regulation and Data Protection Act 2018.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Our Role in processing data

Engaging Eyes Ltd processesservice users, visitors and others, and therefore is a data controller, with the Chief Executive as the person responsible.

Engaging Eyes Ltd is registered as a data controller with the ICO [ZA381958] and will renew this registration annually or as otherwise legally required.

We will process personal data under the following lawful basis:

- For individual clients (I.e. parents) we process personal data on the basis of a contract we have with the client to provide them a service. In this scenario Engaging Eyes Ltd are the data controller
- For organisational clients (I.e. schools) we process personal data on the basis of a public task, schools have a public task to teach children which our software does. The expectation of our relationship with the school is they have the right justification for adding pupils' data into our system and they have provided parents information on our privacy policy or directed them to our website. In this scenario Engaging Eyes Ltd are the data processor.
- For organisational partners (schools who are using our software and in lieu of payment are contributing research data), we process data on the basis of consent. We rely on schools who have partnered with us to gather consent from parents for their children's data to be processed by us. In this scenario, Engaging Eyes Ltd is a data controller.
- For Engaging Eyes Ltd own functions (HR, payroll, marketing), our lawful basis is a contract of employment, legal obligations as an employer, consent or legitimate interest. Engaging Eyes Ltd is the data controller.

3. Roles and Responsibilities

This policy applies to **all staff** employed by Engaging Eyes Ltd and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

3.1 Directors

The directors have overall responsibility for ensuring that our organisation complies with all relevant data protection obligations.

3.2 Data Protection Officer

As a non-statutory body, there is no legal requirement for a dedicated data protection officer. The chief executive will oversee all data protection matters and ensure compliance with the legislation.

Engaging Eyes Ltd is supported by a specialist data protection team at Global Policing who will be called upon, should the matter need specialist support. Global policing has assisted in the production of policy and procedures.

3.3 Chief Executive

The Chief Executive acts as the representative of the data controller on a day-to-day basis. Currently the Chief Executive is also the Executive Director of Engaging Eyes Ltd.

3.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the organization of any changes to their personal data, such as a change of address
- Contacting the Chief Executive in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

4. Collecting personal data

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

5. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a service user that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and service users– for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data processing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our service users or staff.

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

6. Subject Access Requests and Other Rights of Individuals

6.1 Subject Access Requests

Subject access requests must be submitted in writing, either by letter, email or fax to the Executive Director. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the Executive Director.

6.2 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the user or another individual
- Would reveal that the service user is at risk of abuse, where the disclosure of that information would not be in the service user's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the service user

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

6.3 Recording Subject Access Requests

A record will be kept of all Subject Access Requests and logged on the SAR database. This SAR folder and database will be securely stored on site.

A file is to be created for each subject access request and in it should be the following information: -

- Copies of the correspondence between the organisation and the data subject, and between the organisation and any other parties.
- A record of any telephone conversation used to verify the identity of the data subject
- A record of the decisions and how the organisation came to those decisions
- Copies of the information sent to the data subject. For example, if the information was anonymised, keep a copy of the anonymised version that was sent to the data subject.

The file will be kept for one year and then securely destroyed.

When the request has been completed, the record of the request will be closed in the database.

6.4 Other Data Protection Rights of the Individual

Individuals should submit any request to exercise these other data protection rights of the individual (See Appendix 5) to the CEO If staff receive such a request, they must immediately forward it to the CEO

7. Photographs, Videos, and Audio Recordings

As part of our organizational activities, we may take photographs and record images of individuals within our service criteria.

We will obtain written consent from service users for photographs and videos to be taken for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video could be used to service user.

Uses may include:

- Within the organisation, on notice boards and in organisational magazines, brochures, newsletters, etc.
- Outside of the organisation by external agencies such as the church, newspapers, and marketing campaigns
- Online on our organisation website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

Please note as part of our services schools may audio record children reading so that they have the ability to play the recording back, helping children to learn. These recordings are solely used for this purpose and will not be used for anything else. They are managed by the schools via our software; the schools make their own decisions on how to retain the recordings. Engaging Eyes Ltd does not keep any copies of these recordings beyond the contractual relationship with the client School or parent.

8. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Liaising with a suitably qualified DPO when required, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- Completing data protection impact assessments where the organisation's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our organization and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

9. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the main office
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff and service users are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff or service users who store personal information on their personal devices are expected to follow the same security procedures as for centre-owned equipment (see our IT Acceptable Use Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

10. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the organisation's behalf. If we do

so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

11. Personal data breaches

The organisation will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a organisational context may include, but are not limited to:

- A non-anonymised dataset being obtained without permission from our computers.
- Safeguarding information being made available to an unauthorised person.
- The theft of an organizational laptop containing non-encrypted personal data about service users.

12. Training

All staff are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the organisation's processes make it necessary.

13. Monitoring arrangements

The Chief Executive is responsible for monitoring and reviewing this policy.

This policy will be reviewed every two years.

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- Data protection breaches could be caused by a number of factors. Some examples are:
    - Loss or theft of user, staff or director data and/ or equipment on which data is stored;
    - The sharing of system passwords
    - Inappropriate access controls allowing unauthorised use;
    - Equipment Failure;
    - Human Error;
    - Unforeseen circumstances such as fire or flood;
    - Hacking;
    - 'Blagging' offences where information is obtained by deception.
- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the CEO.
- The CEO will investigate the report, and determine whether a breach has occurred. If a breach has occurred, the CEO will consult the external DPO. To decide, the CEO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO and CEO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the designated, protected folder on Global Policing systems.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the designated, protected folder on Global Policing's system.

Review and Evaluation

The Chief Executive will review what happened and how it can be stopped from happening again and this will happen as soon as reasonably possible. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Actions to Minimise the Impact of Data Breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records):-

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the CEO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the CEI will ask the IT Manager to recall it
- In any cases where the recall is unsuccessful, the CEO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The CEO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The CEO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Appendix 2

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership

	• Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Appendix 3

Data Protection Principles

The DPA is based on data protection principles that our organisation must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how **Dyslexia Gold** aims to comply with these principles.

Appendix 4

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the organization holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Appendix 5

Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)