EasyPeasy Data Protection Impact Assessment

Step 1: The need for a DPIA

In this section, we explain broadly what we aim to achieve with EasyPeasy and what type of processing it involves.

EasyPeasy is an app-based programme for parents & carers of children from 0-5 that improves the Home Learning Environment and is proven to close early gaps in child development. It is backed by rigorous independent evaluation. The programme can be delivered by Local Authorities as an early intervention strategy, a universal or a targeted-selected programme e.g. for low-income families. It is primarily delivered in the home of the family and used independently, but can also be integrated into early years settings and used by practitioners.

This DPIA is designed to help you understand how and why we process data and to provide details about our data protection systems.

We collect and process personal data from registered users of the EasyPeasy app, as well as practitioners who sign up for our Practitioner Training sessions. Our activities include monitoring of user data, and in some cases, it also involves the processing of 'special-category' data (i.e. ethnicity) and data concerning vulnerable data subjects (i.e. children's first names and dates of birth). In some cases, we also combine data from multiple sources (i.e. matching user postcodes to LSOA areas from the ONS Income Deprivation Affecting Children Index).

EasyPeasy is available directly to individual users, as well as through partnerships with organisations where the full & free version of the app is made available to specific communities. In the case of the latter, we also process user data to make decisions about eligibility for access to the full & free EasyPeasy offer (i.e. only users with postcodes within a local area may be eligible to access a locally supported EasyPeasy offer).

The reasons that we process user data are to ensure that we can deliver the service to our users, and that we can personalise and localise the service to improve its relevance and impact for our users, as well as ensuring that we are supporting equal opportunities. We process data on the bases of explicit consent, legitimate interests, and contractual necessity.

Step 2: Description of the processing

Nature of the processing

In this section, we set out how we collect, use, store and delete data. We identify the sources of data we collect, who it is shared with, and cover any data processing that is 'high risk'.

How we collect data/sources of data

We collect data in the following ways:

- Direct interactions with users e.g. when users create an account or contact us with a question or issue.
- Using automated technologies e.g. cookies or similar technologies when visitors use the website and the app.
- From third parties e.g. from our third-party analytics provider.

How we use data

The main use of data is to allow account creation and to provide a personalised experience based on a user's interests and the age of their child. We also provide an email newsletter for our users. All email newsletters have an unsubscribe link and all opt-outs are actioned and respected. We do not carry out any behavioural advertising.

We use data for the following purposes:

- To register users who choose to create an account with us.
- To manage our relationship with customers (e.g. responding to questions, complaints, asking users to take a survey).
- To administer and protect our business, website and app (e.g. system maintenance and support, fixing problems, hosting of data).
- To deliver app content and measure and understand the engagement rates.
- To carry out data analytics to improve our app, products, marketing and customer experience in our app.
- To provide email newsletters to users who have subscribed to this service.
- To verify user identity and provide a secure platform.
- To comply with regulatory or legal obligations.
- To enable users to create/edit/delete content and comments.
- To enable users to like and favourite content.
- To enable users to report content and comments that they feel are inappropriate.
- To enable users to block other users.
- To enable users to share content on social media sites.
- To collect basic demographic data during onboarding, including parent/carer age range, gender and ethnicity, and the child's name, gender, and information on whether they were born prematurely (and, if so, by how many weeks).

These data points enable us to improve the personalisation, inclusivity, and equity of the EasyPeasy experience and support Local Authorities with impact evaluation and equal opportunity monitoring.

Cookies

Our website uses cookies for a range of functions outlined below.

- Account authentication
- Cookie consent
- Usage analytics

We have put in place a cookie consent tool which explains the cookies we use and requests consent to these. We also have a cookie policy which explains in more detail the types of cookies we use and the purposes we use them for. The consent tool is available at the point of website entry.

Storage and deletion

User data is stored in Amazon Web Services in the eu-west-2 region, which is in the London, UK area.

User Generated Content (UGC) can include images and GIFs that are stored with a third-party Content Delivery Network (CDN).

Some pseudonymised analytics data is stored in the USA.

Data sharing

Data-sharing practices are conducted in accordance with our RoPA, which details security measures, data handling procedures, and compliance standards. Data is shared for routine data processing necessary to deliver the service.

Our hosting provider (Amazon Web Services) provides the infrastructure we use to keep all of our user data. They have no direct access to the data stored.

We make use of a recommender system provided by a third party. The provider acts as our processor and all user data that they process is pseudonymised.

We make use of third party analytics providers to measure user interactions with our website and app. This is so that we can check the quality and effectiveness of our service and ensure it meets the needs of the user. Our analytics providers use cookies and similar technologies to collect information about user interactions. This includes data about the user's device or browser, their on-site activities, and a portion of the user IP address. The

providers act as processors and all user data that they process is pseudonymised. These reports don't identify the users - they are aggregated information about all our users.

Our analytics providers don't use any of this information for their own purposes - they act as our processor and only operate on our instructions. This processing is carried out in the EU.

We use a third party notification service to provide users with notifications on their device. To make use of this service, certain personal data is transferred to the provider (e.g. 'Hi, Jane'). This processing is explained in our privacy notice.

As part of our partnerships with organisations, we prepare usage reports that aggregate relevant user data for analysis. No PII is shared in these reports.

We use a third party tool for conducting surveys. This provider acts as our processor and does not have access to the answers users give during this optional questionnaire. The survey results are aggregated to help us understand the impact our service is having on building parents' and carers' confidence and knowledge of child development, as well as on improving the home learning environment. We also collect some basic demographic data in this survey which is designed to help us monitor and ensure equality and diversity.

Profiling

We perform profiling on users to show the most useful parenting advice to each user. This is done by asking which topics the user is interested in, the date of birth of their child, and by tracking the content the user views. We then recommend similar content that is age-appropriate for the user's child. The child's date of birth is never shared or processed with third parties.

We operate a moderation system to ensure that no harmful or offensive content is created, shared, or viewed on the platform. It includes a set of Community Guidelines that all users must agree to and adhere to, reviews of all newly published content by our Moderation Team, and a reporting system that allows any user to flag a potentially inappropriate piece of content to our Moderation Team.

Artificial Intelligence (AI) Supported Processing

EasyPeasy makes limited and controlled use of Artificial Intelligence (AI) systems to support operational efficiency, product development, analytics, and content production processes.

AI systems may be used to assist with:

- Draft content creation and summarisation (subject to mandatory human review and accreditation processes)
- Product development, testing, and debugging
- Insight generation and internal reporting

- Workflow automation and operational support

AI systems are not used to make autonomous decisions affecting children, parents, carers, or vulnerable individuals. AI outputs are advisory only and are always subject to human oversight.

Where AI tools process personal data, this is conducted in accordance with UK GDPR, Article 28 contractual safeguards, and EasyPeasy's AI Policy. Personal data is not entered into public or consumer AI tools. Any AI system that processes personal data is subject to:

- A documented security and AI risk assessment
- A Data Protection Impact Assessment (where required)
- A Data Processing Agreement with the provider
- Data minimisation controls and configured retention restrictions
- Prohibition on model training using client or user data

AI governance, oversight, and approval processes are defined in EasyPeasy's Artificial Intelligence (AI) Policy and are reviewed periodically by the DPO and CEO.

Advertising

We do not allow advertising on our website or app.

Security measures

Monitoring and moderation measures are guided by our RoPA to ensure consistent and secure data processing practices. These measures include regular reviews and checks to mitigate any potential gaps, ensuring compliance with data protection standards and transparency in data handling. We use the following security measures for our infrastructure:

- We use a market-leading third party to handle user logins, we have no access to passwords.
- We use HTTPS for all network connections.
- We use a Captcha function on our "contact us" page.
- We use a market-leading, reputable web hosting company.
- We have a policy of regularly deleting any files, databases, or applications from our app and website that are no longer in use.
- We follow the least privilege access principle.
- All data is regularly backed up.
- We run regular web security scans to check for website and server vulnerabilities.
- All user data is encrypted.

Scope of processing

In this section, we cover the scope of our data processing including the nature of the data, and any special categories of data that we process. We specify the quantities of data that

we collect and use, set out how long we keep it, and how many individuals are affected across what geographical regions.

This DPIA is closely aligned with our Retention Policy, RoPA, and Privacy Policy, providing a comprehensive framework for data protection and management practices.

Data processed

Identity data:

- Parent/carer: name, email address, username
- Child: first name, gender, and (optional) prematurity status (and number of weeks if premature).

Contact data: email address.
Location data: postcode.
Technical data: IP address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform.
Profile data: User preferences, interests, feedback, and questions as collected through survey responses and onboarding. Demographic information provided at registration, including parent/carer age range, gender, and ethnicity (required fields). Child-related information collected to personalise developmental recommendations.
Usage data: information about how users use our website, app, and services.
Marketing and communications data: a record of users' preferences in receiving marketing from us.

Special categories of personal data

We collect some special category personal data.

- We collect limited special category data relating to ethnicity from parents/carers during onboarding. This data is collected with explicit consent and used solely to monitor and ensure equality, diversity, and inclusion within the EasyPeasy service. It is aggregated and anonymised for analysis and not shared at a personal level.
- The app also collects limited data relating to children (first name, gender, and optional prematurity details) to enable personalisation and developmental relevance of in-app content. This information is used solely within the app and is not shared externally.
- We ask our users to fill in an optional survey about their experience using our app and the perceived impact it has on their relationship with their child and home environment. As part of this survey, we also ask for some basic demographic information about the user, including their ethnicity. As part of our partnership, we will share the aggregated data from this survey to help ensure equality and diversity. This data is not currently shared at a personal level.
- We require a user's child's date of birth in order to show age-appropriate content. This data is not currently shared at a personal level.

Volume of personal data

The volume of personal data to be processed could reasonably grow to be in the millions.

Retention of data

Retention of Data Our data retention practices align with legal requirements, limitation periods, and programmatic needs for impact analysis and operational purposes. Our retention schedule is designed to ensure data is retained only as long as necessary for specific purposes, with secure deletion protocols once retention periods expire. **These retention periods are consistent with our Retention Timetable and are documented within our Record of Processing Activities (RoPA), ensuring alignment across all data policies and compliance with relevant legal requirements.** Below is an overview of key data categories, their retention periods, and the rationale:

1. **User Records and Personal Identifiable Information (PII)**
    - **User Account Preferences & Settings**: Retained for the duration of a user's engagement with the platform or until the child reaches 18 years old. If a child's date of birth (D.O.B) is unavailable, retention is 8 years after registration. The removal of specific PII (password, username, bio, profile image) when the child reaches 8 years (or 8 years post-registration) aligns with the principle of data minimization and privacy protection. This data supports our program impact analysis and data-sharing agreements with Local Authorities (LAs).
    - **Child Identifiers (e.g., Child_ID, Child Name, Family_ID, D.O.B)**: Retained until the child reaches 18 years to facilitate long-term developmental impact tracking and family engagement analysis.
    - **Sensitive Data (Parent Age, Gender, Ethnicity)**: Retained indefinitely to analyse and track program effectiveness and engagement patterns, while ensuring continued anonymization and security measures.
    - **Feedback Data and Skill Improvement Surveys**: Retained indefinitely to evaluate user experience and program impact while maintaining privacy and data security practices.
    - **Ward & Postcode Data**: Retained until the child reaches 18 years, supporting geographical impact analysis.
2. **PII Removal and Data Minimization**
    - **Personal Data Deletion (Password, Username, Bio, Profile Image)**: Removed once a child reaches 8 years old or 8 years after registration if no D.O.B is available, in accordance with data minimization and storage limitation principles.
    - **Regular Review and Secure Deletion**: All data is reviewed periodically to ensure it meets current retention policies and GDPR compliance. Data is securely deleted or anonymized when retention is no longer necessary.

Compliance with GDPR
We adhere to GDPR principles, including data minimization, transparency, and storage limitation, ensuring that personal data is only retained for as long as it serves defined and justified purposes. The retention policy is periodically reviewed to maintain compliance and align with evolving legal and programmatic needs.

Current Approach to Data Minimization
Our data collection and processing strategies prioritise the minimization of personal data to comply with GDPR principles and reduce potential risks to data subjects. The following outlines our consideration and evaluation of alternative data collection and processing methods to ensure that only the necessary data is collected for achieving our defined purposes.

Evaluation and Documentation of Alternatives

1. **User Data**:
    - **Full Name**: Consideration was given to whether initials or pseudonyms could be used instead of a full name for personalization. Our conclusion was to retain the full name to support direct communication and user engagement. However, the data is not validated beyond initial submission, providing flexibility in usage.
    - **Email**: An evaluation considered using in-app messaging as an alternative communication method. However, retaining emails was deemed essential for account communication, especially for user authentication, platform invites, and critical notifications. To enhance data security, email validation measures will be applied where direct platform invites are involved.
    - **Postcode**: We assessed whether using partial postcodes would meet our requirements for personalization and service delivery. Full postcodes are required due to contractual obligations for assigning premium access based on precise geographical data.
    - **Date of Birth**: The potential to collect age ranges instead of full dates of birth was explored. To minimise data while still delivering personalised content, we will reduce the collected data to month and year (mm/yy) instead of exact dates.
    - **Profile Image and Bio**: While these data points enhance user personalization, they are not strictly necessary for service delivery. Users have full control over these fields and can choose whether or not to provide them.
2. **Trainee Data**:
    - **Full Name and Email**: The collection of full names and email addresses is essential for certification and communication with trainees. However, opportunities to minimise data usage through pseudonymization or internal identifiers will be periodically assessed for feasibility.
3. **Client and Staff Data**:

- **Client Name and Contact Information**: Considered using anonymized identifiers for internal management. However, retaining client names and contact information is necessary for maintaining professional relationships and fulfilling contractual obligations.
- **Staff Personal Information**: We adhere to strict retention and usage policies for staff data to comply with employment and legal requirements. Efforts to pseudonymize or limit access are applied where feasible.

4. **Support Requests**:
    - **Personal Data Minimization**: For support requests, consideration was given to using unique identifiers instead of names. However, names and personal emails are necessary for effective communication and resolution of issues. To minimise data, support requests are anonymized or deleted once resolved.

Justification of Chosen Approach
Our chosen data processing approach balances service functionality, personalization, and compliance with legal and contractual requirements. Minimization strategies are regularly reviewed to ensure that data collection does not exceed the purposes for which it is processed. Where possible, we opt for pseudonymization, data aggregation, and optional data fields, while maintaining critical data points necessary for operational, analytical, and impact analysis functions.

Risk Reduction Measures
To mitigate potential risks associated with data processing, we implement robust data security practices, including encryption, access controls, and periodic data reviews. Our approach is guided by the principle of necessity and proportionality, ensuring minimal data retention without compromising service delivery.

Geographical area

The data subjects whose data we process are located in countries around the world where we operate and where the EasyPeasy app is available on the App and Play Stores. The app and all personal data is hosted in the UK.

Context for processing

In this section, we describe the context for processing the data including the nature of our relationship with our users, how much control they have, their expectations for how we process their data, including with reference to children and other vulnerable groups.

Nature of service and users

In the app, users can create an account to view, create and share parenting tips and ideas.

The website includes a “contact us” function which includes a contact form where users provide name, email, subject and message. This aspect of the service is protected by a third

party's Captcha service, which involves the use of cookies or similar technologies. Further details of security measures applied to our processing are provided in Step 2 above.

The app retains content viewing history and we undertake limited profiling activities of users based on activity they undertake when logged in to customer accounts. We use this data along with user preferences, to recommend similar content to these users.

The website contains links to our social media pages and includes functionality which enables users who have external social media accounts to share content on their social media pages. Social media providers linked to by the site are joint controllers for the processing of this personal data.

Users' expectations

We consider that the above processing will be in line with users' expectations. It is clearly explained in our privacy notice, which is written in basic, easy-to-understand language.

Certifications

- Our health content and content production process is accredited by the Patient Information Forum PIF Tick
- We hold Cyber Essentials certification
- We are registered with the Information Commissioner's Office
- We are registered with National Cyber Security Center

Purposes of the processing

In this section, we cover the purpose of our data processing and what the intended effect of our users is.

Aim of our service

Our mission is to support parents to give their children the best start in life.

Intended effect on individuals

We have designed the EasyPeasy app in partnership with parents and partners to help inspire positive interactions between parents and their children through offering fun, engaging activity ideas, and evidence-based tips and advice. This is because we know that positive parent-child interactions are the single biggest influence on children's healthy early development.

Benefits of the processing

There are many benefits to the ways in which we process user data, from ensuring we are able to effectively reach parents and carers with the EasyPeasy app, to providing them with a

secure and personalised service that is relevant and timely to their needs, as well as helping to keep them engaged and develop more positive habits and behaviours with their child.

Step 3: Our consultation process

In this section, we describe when and how we consult with key stakeholders including our end users, and other stakeholder groups to ensure appropriate security and data protection policies and approaches.

We regularly conduct user-testing within the app and consult with parents and professionals within the early years space when evaluating and making decisions regarding personal data and data protection, e.g. when considering the introduction of a new question in our impact survey, or during onboarding. We carefully evaluate the benefits versus risks of asking for additional data from our users and always A/B test new features with these user groups to evaluate them in practice. We discuss the use and impact of data we capture internally and with our partners.

We also encourage users to fill out a survey to help us understand the impact we're having and to understand our audience's equality and diversity. The survey is conducted online with users who have an account.

We encourage users to leave a rating and review on either Google Play Store or the Apple App Store and listen to any feedback we receive, including feedback that relates to the information and data we request from users as well as our privacy and data protection policies.

All of the content produced on the platform is subject to our Community Guidelines, which set out our responsibilities to moderate and ensure the quality of the content on the platform, as well as setting out user (ie parents and carers) responsibilities for child safeguarding. Our content quality assurance process includes accreditation from the Patient Information Forum through the health content quality mark, the PIF Tick. Finally, all content is tagged with appropriate milestones from the internationally recognised child development framework, Ages and Stages.

We note that where residual risks have been identified, we are satisfied that they are limited and appropriate measures are in place to mitigate potential harm.

We continuously incorporate feedback from our consultations with end users, parents, carers, and professional stakeholders into our data processing policies and procedures. For instance, feedback gathered during user-testing has led to modifications in our privacy notice and data minimization practices. Specific examples include refining how optional survey data is collected to enhance user control and updating our user onboarding process based on feedback to improve transparency around data use. We document all feedback

sessions and review their impact on our data policies to ensure a transparent and adaptive data governance approach.

Step 4: Assessment of necessity and proportionality

In this section, we describe our compliance and proportionality measures, in particular our lawful basis for processing, and how it achieves our purpose, and how to stop function creep. We set out our strategies to ensure data quality and data minimisation, how we support individual's rights, and how we ensure other data processors that we work with comply with our policies. We also set out how we ensure GDPR compliance of international transfers and how we safeguard the small number of international transfers that occur within our current data system.

Lawful basis for processing

Our lawful basis for processing data rests on consent, contractual necessity, and legitimate interests:

- **Contractual necessity (Article 6(1)(b) GDPR):** Personal data collected, such as **full name, email, and username**, is necessary for providing personalised services, ensuring secure access to user accounts, and facilitating communication with users. For example, **personal email** is used for important service communications, and **username** and **password** are essential for secure user access and app functionality. This processing is critical to meet user expectations and fulfil contractual obligations as specified in our Terms & Conditions.
- **Consent (Article 6(1)(a)GDPR):** While a specific opt-in checkbox is not used, consent is implied through user acceptance of EasyPeasy's **Terms & Conditions and Privacy Policy** at the point of sign-up. This acceptance covers processing activities related to **personalised content recommendations and app functionalities**, as clearly outlined in our policies. Transparency is maintained by ensuring that users are informed of how their data will be processed as part of the sign-up flow.
- **Legitimate interests (Article 6(1)(f)UK GDPR):** Legitimate interests assessments (LIAs) have been conducted for processing activities such as **app functionality improvements, security monitoring, and essential communications**. For example, **usage data processing** for enhancing app performance is conducted with robust safeguards, such as **encryption and access control**, ensuring minimal risk to user rights and expectations. Users are made aware of these processes in our Privacy Policy.
- **Explicit consent (Article 9(2)(a) GDPR)**: We process special categories of personal data, such as **ethnicity**, where the data subject has given explicit consent for one or more clearly defined purposes. This consent is obtained through an affirmative action, ensuring that users are fully informed of the processing scope and their rights regarding this data. Appropriate safeguards, such as **pseudonymization and encryption**, are in place to further protect the data.

The lawful basis for processing parent/carer age range and gender, and child name, gender, and prematurity information is contractual necessity and legitimate interest to enable service personalisation, developmental tracking, and equality monitoring.

Data Protection Principles Compliance

EasyPeasy is committed to adhering to all GDPR data protection principles, including lawfulness, fairness, transparency, data minimization, accuracy, purpose limitation, integrity, and accountability. Below is a demonstration of how our data processing aligns with these principles, with explicit examples and relevant measures in place:

1. **Lawfulness, Fairness, and Transparency**:
    - All personal data collected and processed is based on clearly defined and documented legal bases as detailed in our Record of Processing Activities (RoPA). For instance, processing **full names and email addresses** for user account creation and communication is based on **contractual necessity or legitimate interests**, as outlined in our user agreements and privacy policies.
    - Transparency is maintained through clear user agreements and privacy policies that explain data processing practices, such as the collection of **ethnicity data for equal opportunity monitoring** using **explicit consent**.
2. **Purpose Limitation**:
    - Personal data is collected solely for specified, legitimate purposes, such as **delivering personalised content, user authentication, and analysing app usage to improve user experience**. Data points such as a child's **date of birth** are used strictly for age-specific content delivery, and **special category data** like **ethnicity** is only used for optional surveys as outlined in our privacy notices.
    - Processing activities are documented and monitored to prevent function creep, ensuring data is used only for the intended and communicated purposes.
3. **Data Minimization**:
    - Our Data Minimization Review has evaluated each data point to ensure only data necessary for service delivery is collected. For example, the collection of **postcode data** is limited to fulfil specific contractual obligations related to geographical services, and **profile images and bios** are optional fields to reduce unnecessary data collection where possible.
    - Minimization measures also extend to reducing the granularity of data where feasible, such as by collecting the **month and year (mm/yy) instead of exact birth dates** for children.
    - The addition of new onboarding fields has been subject to a data minimisation review. All new questions are mandatory only where essential to service personalisation and impact monitoring. The “prematurity” question is optional and collected only where volunteered. Aggregated demographic data will be reviewed quarterly to ensure it remains proportionate to its stated purposes.

4. **Accuracy**:
    - Personal data accuracy is maintained through periodic reviews and user updates. For instance, users can update their **account preferences, email addresses, and contact details** at any time to ensure data remains up-to-date.
    - Any inaccuracies are promptly corrected or deleted upon notification, as required by GDPR's accuracy principle.
5. **Storage Limitation**:
    - Retention periods for personal data are specified and periodically reviewed to align with operational needs and legal requirements. For example, **user data** is retained until a child reaches 18 years of age (or 8 years after registration if no date of birth is provided) to support long-term impact analysis and data sharing with Local Authorities. **PII data**, such as **passwords and usernames**, are removed when a child reaches 8 years old to align with privacy principles.
    - Specific data retention measures, such as **data deletion protocols and anonymization practices**, ensure that data is only retained as long as necessary for its original purpose.
6. **Integrity and Confidentiality (Security)**:
    - Robust security measures are implemented to protect data integrity and confidentiality, including **encryption at rest and in transit, role-based access control (RBAC), regular security audits, and training for personnel**.
    - Access to personal data is limited to authorised personnel and third-party processors who comply with GDPR requirements and data protection agreements, as outlined in our data-sharing protocols.
7. **Accountability**:
    - EasyPeasy maintains detailed records of processing activities, conducts **Data Protection Impact Assessments (DPIAs)** where necessary, and regularly reviews its data processing practices.
    - Compliance with data protection principles is further demonstrated through **legitimate interest assessments, explicit consent mechanisms, and regular audits** to ensure ongoing compliance with data protection laws.
    - AI systems are governed under EasyPeasy's Artificial Intelligence (AI) Policy, which sets out approval, oversight, and risk management processes. AI tools are subject to documented risk assessments and, where applicable, DPIAs. AI outputs remain subject to human review and accountability remains with EasyPeasy staff.

Transparency and data subject rights

Individuals are given information about our processing through our online privacy notice which they are able to review when they create an account. It is also accessible from our app menu and website footer. Our cookie policy contains information about cookies used in the app and on our website. This is accessible through our cookie consent tool and from our website footer.

We explain about individuals' rights in our privacy notice and include an email address which individuals can use to contact us with any questions about their rights and to exercise their rights. Our team members who deal with queries on data protection matters and requests to exercise data subject rights have received basic training on dealing with requests and are familiar with the guidance produced by the ICO.

Processors

We use an accounts and authentication service, a recommendation engine service, multiple analytics providers, a notification service, an image and video processor, a Captcha provider, all of which act as processors. We have entered into Article 28(3) UK GPDR terms with each of these third parties and carried out appropriate security risk assessments.

The Article 28 agreements include a contractual obligation for the processor to use EU SCCs and undertake a risk assessment if or when engaging the services of a sub-processor who is transferring data to a third country.

International transfers

We work with a GDPR compliance provider, Iubenda, to ensure the GDPR compliance of our privacy policy and terms & conditions.

Transfers of data are made in connection with the sharing of personal data with our third-party processors. Our hosting provider keeps user data in the UK. Our analytics providers are based in Europe and North America. Our recommendation service is based in Europe. Our notification service is based in North America.

In all cases where user data is transferred and processed outside of the EU, Standard Contractual Clauses have been reviewed and are in place providing adequate protections for the privacy rights of our users that are GDPR compliant.

Best interests of the child

The app is designed for use by adult parents and carers of 0-5-year-old children, and not designed to be given to a child to use unattended. However, it is possible that a child could see and possibly interact with the app and we have taken actions to mitigate the risks associated with this. Our moderation process and Community Guidelines ensure that content on the platform is safe for and appropriate for children. We do not collect specific information about children beyond their date of birth which we use to show their parents' or carers' content specific for a child of that age.

Data protection impact assessments: We have completed this DPIA which covers all customer data processing activities carried out. We keep this DPIA under review and are aware of the need to update it if we make any changes to our processing of customer personal data. We make the up-to-date version of this DPIA available on request.

Age Appropriate Application

The app is clearly geared towards parents and carers of 0-5 year-olds and holds little entertainment value for children in of itself. Parents and carers are encouraged to put their device down and play the games offline with their children. We only collect and process limited personal data from all users, and our use of data is limited to what people would expect in the context of an online content app. We apply the same standards and carry out the same processing activities in relation to all users.

Transparency

We provide a privacy notice and cookie policy explaining how we use personal data and how cookies are used in our app and on our website. In addition, we provide additional specific bite-sized explanations about how we use personal data at the point at which we collect it.

Detrimental use of data

We do not use personal data in any way which could be detrimental to a child's or any other person's well-being.

Policies and community standards

We follow our terms and conditions and privacy notice and only use data in accordance with these documents. We will delete the accounts of users that do not follow our standards. We will also delete any data collected against their account.

Default settings

As our website only has basic functionality, we do not use privacy settings unless the user creates an account. Account holders' privacy is set as high by default. This means we do not collect more data than is necessary to provide the app service and newsletter service that comes with a user account. User account holder data is not visible to other users.

No cookies (apart from strictly essential cookies) are placed before a user consents to such cookies. All other cookies are set as default to "off".

Data minimisation

We only collect and process the minimum amount of personal data we need for the functioning of the app.

Data sharing

Data is shared with the third parties described under the heading "Data sharing" in Step 2.

Geolocation

We do not collect precise location data from our users. We do ask for a postcode from our users to ensure that we deliver contracts with our local government partners efficiently and

correctly, and so that we are able to effectively monitor our shared reach to low-income households, which is a key part of our social mission and strategic objective.

Parental controls

We have analysed the processing we carry out and do not think that any of it presents a risk which would require us to offer parental controls. Parents or guardians can contact us with any queries they have about our processing of their child's personal data, ask us to delete the personal information we have collected in connection with their child from our records, and exercise rights on behalf of their child. We confirm the identity of the adult as the parent or guardian of the child before carrying out any of the above.

Profiling

We carry out limited profiling activities to provide recommendations of content to users based on their interests and browsing activities.

We do not offer external advertising to users of the service.

Nudge techniques

We do not use nudge techniques to encourage children to provide us with data or consent to the processing of their personal data.

Connected toys and devices

We do not use connected toys or devices in the delivery of EasyPeasy.

Online tools

All emails and our generic e-newsletter contain an unsubscribe link. Users who have registered for an account also have the option to delete their account at any time (subject to limited data retention in line with our retention policy).

Step 5: Identification and assessment of risks

We have carefully reviewed our processing and do not think that we carry out any activities that are likely to pose a significant risk to users. Specifically, we are satisfied, that the processing is not likely to give rise to any of the following harms:

- access to websites offering age-inappropriate content or activities;
- financial harm (eg advertising encouraging inappropriate or excessive spending online);
- grooming or abuse;
- inappropriate sharing of personal information, including via uploading content containing children's personal data;
- access to inappropriate goods;

- discrimination (around price of products);
- harassment, bullying, loss of social standing leading to self-esteem and mental health issues;
- intrusion into private spaces and associated loss of privacy for the child;
- inaccessibility of services or discrimination due to a disability; or
- service lock-in ie: unfair contractual terms.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm Remote, possible or probable	Severity of harm Minimal, significant or severe	Overall risk Low, medium or high
The app is designed for use by adult parents and carers of 0-5 year old children, and not designed to be given to a child to use unattended. However, it is possible that a child could see and possibly interact with the app.. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Remote	Minimal	Low
Gaps in monitoring and moderating data leads to inappropriate content being viewable on the app for periods of time, including by children. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Our failure, or the failure of our users (ie parents and carers) to uphold our Community Guidelines exposes children to harm. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Data Retention Beyond Necessity. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Data Minimization. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Lack of Explicit Consent for Special Category Data. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Severe	Medium
International Data Transfers. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Access and Data Subject Rights. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Remote	Minimal	Low

Profiling and Automated Decision-Making. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Third-Party Data Sharing Without Adequate Safeguards. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Users registering without full information about data processing. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Unprecedented volume of rights requests leading to non-compliance. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Processing data for secondary incompatible purpose. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Users uploading extra data in free text spaces. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Users not updating personal data. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Data retained too long or deleted early. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Data accessed/lost by external party. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Severe	High
Data accessed/lost by internal party. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Severe	High
Breakdown in internal security controls. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Severe	High
Accidental loss of data. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Severe	High
Processors not complying with obligations. Source of risk includes potential compliance, operational, and corporate impact considerations where relevant.	Possible	Significant	Medium
Processing PII of vulnerable user data shared by an LA partner for the supporting families programme.	Possible	Severe	High

Sharing of PII data from vulnerable users to Client staff/contractors who should not have access	Possible	Significant	High
Collection of additional demographic and child data during onboarding (age range, gender, ethnicity, child name, gender, prematurity)	Possible	Significant	Medium
AI-generated or AI-assisted content may include factual inaccuracies, fabricated information, unsafe or inappropriate advice, or SEN guidance that is oversimplified, incorrect, or insensitive. This could result in misalignment with NHS, EYFS, UNICEF BFI, WHO Code, SEND Code of Practice or other UK guidance, creating safeguarding, reputational, compliance, or legal risks.	Possible	Significant	Medium
AI-assisted recommendations (including pathways, activities, or local service suggestions) may be inappropriate, inaccurate, misaligned to a child's developmental stage, or omit safeguarding-critical information. This may result in reduced effectiveness, parental confusion, or reputational and contractual risk with Local Authorities.	Possible	Significant	Medium
AI-assisted drafting of policies or documentation may introduce incorrect legal interpretations, outdated regulatory references, inconsistencies with UK GDPR or contractual requirements, or drafting errors that could create compliance or legal exposure if not reviewed.	Possible	Significant	Medium
Bias within training data, prompt structures, or datasets used to support AI systems may lead to unequal recommendations, exclusion of certain demographic groups, inaccurate representation, or culturally inappropriate outputs. This may create fairness, equality, or reputational risks.	Possible	Significant	Medium
AI-assisted translation or localisation processes may produce inaccurate, misleading, culturally inappropriate, or safety-critical errors in translated content, potentially altering meaning or reducing	Possible	Significant	Medium

clarity for families.			
Over-reliance on AI-generated outputs or automation may reduce critical human oversight, leading to inappropriate content approval, reduced safeguarding review, or operational errors.	Possible	Significant	Medium
AI tools may increase the sophistication of phishing, impersonation, or social engineering attacks targeting staff or contractors, increasing the risk of unauthorised access, credential compromise, or data breach.	Possible	Severe	Medium–High
AI-assisted cyberattack techniques may increase the scale, automation, or effectiveness of attacks against EasyPeasy systems, potentially bypassing traditional security controls.	Possible	Severe	Medium–High

Step 6: Identification of measures to reduce risk

In this section, we set out measures we have taken to reduce or eliminate medium or high risks identified above.

Risk	Options to reduce or eliminate risk	Effect on risk Eliminated reduced accepted	Residual risk Low medium high	Measure approved Yes/no
The app is designed for use by adult parents and carers of 0-5 year old children, and not designed to be given to a child to use unattended.	All communication and references within the app are directed towards parents and carers, ensuring that the intended audience is explicitly clear. Personalisation within the app focuses solely on the parent's name and does not reference the child's name, even if such information is provided by the user.	Reduced	Low	Yes

Gaps in monitoring and moderating data leads to inappropriate content being viewable on the app for periods of time, including by children.	All newly published user generated content and comments are flagged to our Moderation team immediately through automated notifications for review. Notifications are monitored during our working hours which are Monday - Friday 9.00-18.00	Reduced	Low	Yes
Our failure, or the failure of our users (ie parents and carers) to uphold our Community Guidelines exposes children to harm.	Through our Community Guidelines we make clear to users that content on the EasyPeasy app includes user generated content that is the responsibility of the content creator. We make clear that content may contain medical advice that is incorrect, and that parents and carers should always consult their doctor for medical advice, and call 999 in the case of an emergency.	Reduced	Low	Yes
Data Retention Beyond Necessity	Implement automated deletion processes; regular audits	Reduced	Low	Yes
Data Minimization	Regularly review and limit data collection	Reduced	Low	Yes
Lack of Explicit Consent for Special Category Data	Ensure clear and explicit consent for special category data	Reduced	Low	Yes
International Data Transfers	Review SCCs and international transfer compliance	Reduced	Low	Yes
Access and Data Subject Rights	Enhance user interfaces for easy data requests	Reduced	Low	Yes

Profiling and Automated Decision-Making	Provide opt-in options for profiling	Reduced	Low	Yes
Third-Party Data Sharing Without Adequate Safeguards	Audit third-party contracts and enforce DPAs	Reduced	Low	Yes
Users registering without full information about data processing	Provide clear privacy notices and opt-in consent mechanisms	Reduced	Low	Yes
Unprecedented volume of rights requests leading to non-compliance	Implement a scalable system to handle individual rights requests	Reduced	Low	Yes
Processing data for secondary incompatible purpose	Ensure data is only processed for agreed purposes	Reduced	Low	Yes
Users uploading extra data in free text spaces	Limit data inputs and provide guidance	Reduced	Low	Yes
Users not updating personal data	Encourage users to update information	Reduced	Low	Yes
Data retained too long or deleted early	Regularly audit data retention schedules	Reduced	Low	Yes
Data accessed/lost by external party	Strengthen external security controls	Reduced	Medium	Yes

Data accessed/lost by internal party	Ensure strict internal access controls	Reduced	Medium	Yes
Breakdown in internal security controls	Regularly test security systems	Reduced	Medium	Yes
Accidental loss of data	Implement disaster recovery plans	Reduced	Medium	Yes
Processors not complying with obligations	Regular audits of processors	Reduced	Low	Yes
Accidental sharing of vulnerable families PII	Restricted access to data, regular audit of process and regular training for all users how access or manage this data	Reduced	medium	Yes
Accidental sharing of vulnerable families PII externally	Restricted access to data, regular audit of process and regular training for all users how to access or manage this data. Password protected documents	Reduced	medium	Yes
Potential sensitivity around new demographic and child-related fields	Include clear consent statements and “why we ask” explanations in onboarding; pseudonymise data in reports; provide easy access to privacy notice; include opt-out for optional questions	Reduced	Low	Yes
AI-generated or AI-assisted content may include inaccuracies, unsafe guidance, biased examples,	Mandatory human review prior to publication; expert accreditation and PIF Tick process maintained; documented compliance	Reduced	Low	Yes

or misalignment	checklist covering health, safeguarding and SEN standards; use of approved reference materials and structured prompts; quarterly AI QA audits and annual governance review.			
AI-assisted recommendations may be inappropriate, inaccurate, misaligned to developmental stage, or omit safeguarding-critical information	Deployment of rule-based guardrails around recommendations; combination of ASQ milestone logic with human oversight; validation of outputs prior to deployment; annual audit of recommendation outputs against developmental frameworks.	Reduced	Low	Yes
AI-assisted drafting of policies or documentation may introduce incorrect legal interpretations, outdated references, or inconsistencies with GDPR or contractual obligations.	All AI-assisted policy drafting subject to DPO approval and legal review where required; version-control log maintained for AI-assisted documents; annual policy review cycle.	Reduced	Low	Yes
Bias in AI-supported outputs or datasets may lead to unequal recommendations, exclusion of demographic groups, or culturally inappropriate outputs.	Regular dataset review and refresh; bias and fairness testing of outputs; annual AI ethics review; internal validation prior to deployment.	Reduced	Low	Yes

AI-assisted translation may produce inaccurate, misleading, culturally inappropriate, or safety-critical errors in translated content.	Use of validated glossary and safeguarding terminology list; structured prompts; user feedback reporting loop; periodic review of translated outputs; correction workflow for identified issues.	Reduced	Low	Yes
Over-reliance on AI outputs may reduce appropriate human oversight, increasing risk of operational, compliance, or safeguarding error.	AI outputs designated as advisory only; mandatory human-in-the-loop approval processes; clear staff accountability retained; staff training on responsible AI use.	Reduced	Low	Yes
AI-enabled phishing, impersonation, or automated cyberattack techniques may increase risk of unauthorised access, credential compromise, or data breach.	Enforcement of MFA and RBAC; ongoing phishing awareness training; monitoring of emerging AI-enabled threats; regular patching and secure configuration; integration into incident management process.	Reduced	Low	Yes

Ongoing Monitoring and Assurance Measures

EasyPeasy conducts a monthly data privacy and security oversight meeting, attended by key team members, including the Data Protection Officer (DPO) and relevant stakeholders. During these meetings, we review and update the following critical areas:

- **Data Privacy Policies and Procedures**: Review and update policies as needed, ensuring they align with evolving legal and operational requirements.
- **Risk Register and Mitigation Actions**: Cross-referencing the DPIA risks with the organisational risk register to maintain consistency and update risk mitigation measures.
- **Sub Processors**: Regular reviews of third-party data processors to ensure ongoing compliance with GDPR and our data protection standards.

- **User Data Requests and Security Metrics**: Monitoring user data requests and tracking key performance indicators (KPIs) for data security and privacy.

Actions identified during these meetings are documented, tracked, and addressed to ensure the effectiveness of risk mitigation measures. This periodic review strengthens our data protection practices and assures compliance with ICO guidelines.

Staff Training and Development
To support compliance, all EasyPeasy staff undergo regular data protection and security training, consistent with ICO recommendations for organisations of our size. Training includes:

- **New and Ongoing Training**: Regularly updated sessions for all new staff, with refresher courses for existing team members.
- **Specialised Training**: Focused sessions for team members with data handling responsibilities, ensuring they stay up-to-date with the latest data protection requirements and best practices.
- **Training Plan Oversight**: Training is reviewed periodically to ensure it remains relevant and effective, adapting to changes in data protection laws or our operational practices.

Step 7: Review and sign off

This DPIA will be kept under review by:

- Martin Vowles, EasyPeasy DPO

Last reviewed February 2026

Next scheduled review: *February 2027*