Data Protection Impact Assessment (DPIA)

IG Form

A DPIA:-

a. Is a process that assists organisations in identifying and minimising the data protection/privacy risks of new projects or policies.

b. Involves working with internal and external stakeholders to identify and reduce privacy risks.

c. Will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

d. Benefits organisations by producing better policies and systems and improving the relationship between organisations and individuals.

e. Is an integral part of taking a privacy by design approach

When completing this form please refer to the Guidance at the end of this document.

1. Identify the need for a DPIA

Please explain in the box below:-

- ✓ What processing will be undertaken
- ✓ What the project aims to achieve and its purpose
- ✓ The necessity and proportionality of the processing in relation to its purpose
- ✓ The benefits of the project (to the organisation, individuals and others)
- ✓ Why the need for a DPIA was identified

You may at this stage wish to add relevant documents, such as a project proposal

Use of new data processor , which provides software that allows our Education staff to more effectively produce teaching evidence, assessments and reports and to track individual student progress

Processing :-

- Input of information into assessment frameworks/ increased input depending on achievement level
- Data reporting
- Data of achievement of vulnerable groups-anonymous

Aims of project :-

- Tracking student progress
- Assessment of skills
- Demonstration of progress for LA funding requirements
- Cohesive, transdisciplinary assessment from 5 years to 25 years
- All departments to use the same system to demonstrate progress; staff can refer to assessment frameworks from other departments

Necessity and proportionality :-

- Personal data linked only to achievement, tracking progress; ensures that no individual or vulnerable group gets 'left behind'.
- Photo and film evidence-purely to evidence achievement over time
- Photo permissions: Quality Assurance process to assure other students are only included in students' photos if have relevant permissions and relevant to learning targets.

Benefits of the project :-

- See above

Need for DPIA :-

- Information about individuals will be disclosed to an organisation which previously did not have access to this information
- Using information about individuals in a way it is not currently used

2. Describe the information flows

Please describe in the box below:-

- ✓ The information flows:-
  - ~ What information is used
  - ~ What it is used for
  - ~ Who it has been obtained from
  - ~ Who it will be disclosed to
  - ~ Who will have access to it
- ✓ The collection, use and deletion of personal data
- ✓ How many people are likely to be affected by the project

You may at this stage wish to refer to a flow diagram or other way of explaining data flows

What information is used

- Education, Health and Care Plan (EHCP) Learning Outcomes and small steps per learner
- Personal data from our current MIS system (Databridge)

What it is used for:-

- Tracking small steps of achievement/ progress against a range of skills including EHCP Learning Outcomes

Whom/ where it has been obtained from:-

- Current MIS system
- EHCP

Who it will be disclosed to:-

- The student her/himself, staff, parents/ carers, external professionals e.g. at annual reviews.

Who will have access to it:-

- Administrative staff at The Data Processor Academic
- The student her/himself, staff
- Parents/ carers through the Parent Portal when this function is introduced in the future. A parent can only access information/ evidence of their own child's progress. Parental permissions apply.

The collection, use and deletion of personal data :-

- Photo/ video is automatically deleted off the portable electronic device, as it's uploaded into the The Data Processor Academic cloud storage
- Data Processor's Data Protection Policy

  "[The data processor] will only hold such personal data as is required to fulfil its obligations under this contract and that once this data is no longer required for this purpose, it will be deleted.

  [The data processor] will delete all assessment data five years after the relevant school year-end. However, in order to fulfil its obligations under its contract with schools, [The data processor]g will retain all media and associated metadata for five years after the last User tagged to that media has been Archived. Then it will be deleted."

How many people are likely to be affected by the project :-

- Students
- Staff
- Parents

3. Identify the privacy and related risks

In the table below please identify the key privacy risks and the associated compliance and corporate risks (add extra rows as needed). Larger-scale PIAs (Protection Impact Assessment) might record this information on a more formal risk register.

Some will be risks to individuals – for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy. Some risks will be to the organisation - for example damage to reputation, or the financial costs or a data breach. Legal compliance risks include the DPA (Data Protection Act), PECR (Privacy and Electronics Communication), and the Human Rights Act.			
Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
1. Does The Data Processor use adequate security?	Information kept on the Data Processor's server may not be as secure as on Young Epilepsy's	Security breach	IG Breach Damage to reputation ICO sanction/fine
2. Are there appropriate safeguards for transmitting information over the internet?	Information may be hacked/ intercepted	Security breach	The Data Processor clearly state that the risk of transmission will lie with Young Epilepsy.
3. Does the Data Processor use appropriate security and access controls?	Information may not be appropriately secure	Security breach	IG Breach Damage to reputation ICO sanction/fine
4. Are the Data Processor appropriately train and vet staff	The Data Processor staff may misuse data	Security breach	IG Breach Damage to reputation ICO sanction/fine
5. Is the Data Processor a suitable and trusted partner	Misuse or breach of data	Security breach	IG Breach Damage to reputation ICO sanction/fine
6. Does the Data Processor comply with the GDPR and the Student Records privacy notice?	Misuse or breach of data	IG breach	IG Breach Damage to reputation ICO sanction/fine

7. Will the Data Processor's information be accurate and up to date?	Inaccurate personal data	GDPR/ DPA 2018 breach	The Data Processor statement:- *"It is the responsibility of the School to ensure that the data in The Data Processor is always current".*
8. Are there appropriate security processes in place for the access of third parties to the data? Statement from the Data Processor *"We may use independent contractors to provide services on our behalf. Such third parties may have access to personal information in the course of providing services on our behalf".*	Third party access	Security breach	IG Breach Damage to reputation ICO sanction/fine
9. Could links to third party websites on The Data Processor cause security issues? The Data Processor statement *Our website may contain links to other sites for your convenience. In most cases, those sites are not under our control, and they have their*	Misuse or breach of data	Security breach	The Data Processor clearly states:- *We bear no responsibility for linked websites and provide these links solely for your convenience and information".*

own policies regarding privacy, which you should review before using them			
10. Will adverts on the Data Processor have a detrimental effect? The Data Processor statement *Currently, The Data Processor does not work with third parties that provide advertisements to our site. This could change in the future, and if it does, a revised privacy policy will be issued".*	Misuse or breach of data	Security breach	IG Breach Damage to reputation ICO sanction/fine

4. Identify privacy solutions

In the box below explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy.

Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project that is still effective.

Result - is the risk eliminated, reduced, or accepted?

Evaluation - is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Risk	Solution	Result	Evaluation

1. Does The Data Processor use adequate security?	a. Review of security provisions by IT team (see IG Compliance Analysis form). b. Statement by The Data Processor *'The data held by [the Data Processor] is protected from exposure by multiple layers of firewalling, authentication, intrusion detection and physical access control".* c. Include as a contractual requirement	In the absence of a single sign on, Education team have requested password complexity as follows.12 characters in length • At least upper and lower case • At least 1 number or special character	All possible security steps taken
2. Are there appropriate safeguards for transmitting information over the internet?	a. Statement from the Data Processor *'all data will be encrypted during transmission and processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage"*	IT project lead has established the security of the cloud servers used and the intent in the disclaimer for responsibility for security.	All possible security steps taken
3. Does the Data Processor use appropriate security and access controls?	a. Review of security provisions by IT team b. Include as a contractual requirement	In the absence of a single sign on, Education team have requested password complexity as follows.12 characters in length • At least upper and lower case	All possible security steps taken

		• At least 1 number or special character IT project lead has established the security of the cloud servers used and the intent in the disclaimer for responsibility for security	
4. Are the Data Processor's staff appropriately trained and vetted?	a. Education to obtain a statement from the Data Processor confirming this b. Include as a contractual requirement	The Data Processor has confirmed that 'the people processing the data are subject to a duty of confidence	Forms part of contract. All possible steps taken
5. Is the Data Processor a suitable and trusted partner?	a. Due diligence to be undertaken by Education team b. Process for review by Education team	The YE Lead Ambassador has:- • Undertaken due diligence • Ensured that the contract clearly states that the Data Processor:- ~ Is the data processor; ~ Will only process data under Young Epilepsy's instructions; ~ Will at all times uphold Young Epilepsy's and the GDPR's standards; and ~ Meets the necessary standards needed for a data processor contract.	Sufficient steps undertaken
6. Does The Data Processor comply with the GDPR and	a. See statement from The Data Processor	The Data Processor have confirmed this	Forms part of contract. All possible steps taken

the Student Records privacy notice?	b. Include as a contractual requirement		
7. Will the information on the Data Processor be accurate and up to date?	a. IT team to set up a daily secure export/ import from Databridge to YE/ YE to EARL b. Quality Assurance processes set up by Education Senior Managers and Lead The Data Processor Ambassador	The YE Lead Ambassador/ Administrator has established processes to • ensure daily synchronisation with Databridge MIS to remove/supress for Leaver accounts • ensure synchronisation with Databridge MIS to add new starter accounts	System in place. Only risk is human error
8. Are there appropriate security processes in place for the access of third parties to the data?	a. Statement from The Data Processor "Any personal information that we provide to such third parties is protected under a confidentiality agreement. Such third parties will take commercially reasonable measures to keep your personal information safe, private and secure. b. Include as a contractual requirement	• The Data Processor has confirmed that they will 'only engage sub-processors with the prior consent of Young Epilepsy and under a written contract' • See above statements on passwords and cloud servers	All reasonable steps taken
9. Could links to third party websites on The Data Processor cause security issues?	a. Education to ensure its staff are trained on whether links are appropriate to access b. The Data Processor Lead Ambassador-to review	Risks minimised	All reasonable steps taken

	privacy policy of linked websites		
10. Will adverts on The Data Processor have a detrimental effect?	a. Education to ensure its staff are trained on how to manage adverts	Risks minimised	All reasonable steps taken

5. Sign off and record the DPIA outcomes

Make sure that the privacy risks have been signed-off by a member of the Exec team. This can be done as part of the wider project approval.

A PIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

Publishing a PIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.

Risk	Approved solution	Approved by who?
1. Does The Data Processor use adequate security?	Security levels reviewed and approved by IT	IT project lead
2. Are there appropriate safeguards for transmitting information over the internet?	Encryption level reviewed and approved by IT	IT project lead
3. Does the Data Processor use appropriate security and access controls?	Security and access controls reviewed and approved by IT	IT project lead
4. Are The Data Processor staff appropriately trained and vetted?	Included as contractual term with The Data Processor	Data Protection Officer/YE Lead Ambassador
5. Is The Data Processor a suitable and trusted partner?	Due diligence undertaken and status confimed	YE Lead Ambassador

6. Does The Data Processor comply with the GDPR and the Student Records privacy notice?	Included as contractual term with The Data Processor	Data Protection Officer/YE Lead Ambassador
7. Will the information on The Data Processor be accurate and up to date?	Role of YE Lead Ambassador/Administrator established to ensure this happens	YE Lead Ambassador
8. Are there appropriate security processes in place for the access of third parties to the data?	Contractual term that third parties will only be given access with Young Epilepsy approval	Data Protection Officer/YE Lead Ambassador
9. Could links to third party websites on The Data Processor cause security issues?	YE Lead Ambassador/Administrator to provide guidance to Education team	YE Lead Ambassador
10. Will adverts on The Data Processor have a detrimental effect?	YE Lead Ambassador/Administrator to review and provide guidance to Education team	YE Lead Ambassador

6. Integrate the PIA outcomes into the project plan

In the box below please identify who is

- ✓ Responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork
- ✓ Responsible for implementing the solutions that have been approved
- ✓ The contact for any privacy concerns that may arise in the future
- ✓ Responsible for monitoring that these actions are undertaken

It may be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

Action to be taken	Date for completion of actions	Responsibility for the actions
All DPIA outcomes have been incorporated into the plan, as detailed above and in the IG Compliance Analysis form.		
Name of contact for future DPIA concerns (please detail below)		
YE Lead Ambassador/Administrator		

Guidance on completion of a DPIA

Please find below the following:-

- Examples of projects that may need a DPIA
- Guidance on consultation
- Guidance on completing each section of the form
- General Data Protection Regulation (GDPR) issues to be considered
- Human Rights issues to be considered

Projects that may need a DPIA

Projects that will need a PIA include (but are not limited to) the following:-

- ✓ A new IT system for storing and accessing personal data.
- ✓ A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- ✓ A proposal to identify people in a particular group or demographic and initiate a course of action.
- ✓ Using existing data for a new and unexpected or more intrusive purpose.
- ✓ A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding automatic number plate recognition capabilities to existing CCTV).
- ✓ A new database which consolidates information held by separate parts of an organisation.
- ✓ Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

Consultation

Consultation is an important part of a DPIA and allows people to highlight privacy/data protection risks and solutions based on their own area of interest or expertise. It can happen at any point in the DPIA process.

Internal consultation

It is important to ensure that all relevant perspectives are taken into account. The people to be consulted within an organisation may include:-

- ✓ Project management team
- ✓ Data protection officer
- ✓ Engineers, developers and designers
- ✓ Information technology (IT)

- ✓ Procurement
- ✓ Potential suppliers and data processors
- ✓ Communications
- ✓ Customer-facing roles
- ✓ Corporate governance/compliance
- ✓ Corporate governance/compliance
- ✓ Researchers, analysts, and statisticians
- ✓ Senior management

External consultation

This provides the opportunity to get input from the people who will ultimately be affected by the project and to benefit from wider expertise. There should be two main aims:-

1. It enables an organisation to understand the concerns of those individuals.
2. It will also improve transparency by making people aware of how information about them is being used.

The ICO states that although not always suitable organisations should not ignore the importance of external consultation and should it always be considered.

How extensive the consultation needs to be will be driven by the types of risk and the numbers of people affected. The consultation should be designed so that individuals can have a meaningful impact on the project, but organisations should make it clear as to what aspects of the project are open to change and which are less so.

Effective external consultations should:

1. Be timely – at the right stage and with enough time for responses.
2. Be clear and proportionate.
3. Have reach and representation – so that those likely to be effected have a voice.
4. Ask objective questions and present realistic options.
5. Provide feedback – so that those participating get feedback at the end of the process.

Completing the form

1. Identify the need for a DPIA

   a. Complete the DPIA screening form to identify a proposal's potential impact.
   b. Begin to think about how project management activity can address privacy issues.
   c. Describe the overall aims of the project.
   d. Start discussing issues with stakeholders.

   This should be completed during the planning stage of a project, so that the development process can take account of any concerns.

2. Describing information flows

a. Explain how information will be obtained, used, and retained – this can be based on, or form part of, a wider project plan.
b. Potential future uses should be identified even if they are not immediately applicable.
c. The people who will use the information should be consulted on the practical implications.

3. Identifying privacy and related risks

a. Record the risks to individuals, including possible intrusions on privacy.
b. Assess the corporate risks, (such as regulatory action, reputational damage, and loss of public trust).
c. Conduct a compliance check against the GDPR and other relevant legislation.
d. Maintain a record of the identified risks.

This will help identify the likelihood and severity of the risks, and if necessary make changes to the project.

Risks to individuals may include

- ✓ Information being shared inappropriately – if there are inadequate disclosure controls
- ✓ Information being used for different purposes without people's knowledge – if the context in which information is used or disclosed changes over time.
- ✓ An unjustified intrusion on privacy – if new surveillance methods are used.
- ✓ Being intrusive – if measures taken result in the collecting information.
- ✓ A greater amount of information being kept than expected – if datasets are shared or merged
- ✓ Removal of anonymity – if identifiers are collected and linked. (Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.)
- ✓ Security risks – if information is collected and stored unnecessarily, or is not properly managed so that duplicate records are created.
- ✓ Kept for longer than necessary - if a retention period is not set.

Corporate risks may include:-

- ✓ Sanctions, fines and reputational damage – if breach the GDPR.
- ✓ People avoiding engaging with the organisation – if the use of biometric information or potentially intrusive tracking technologies increases concerns.
- ✓ Less useful records – if information is collected and stored unnecessarily, or is not properly managed so that duplicate records are created
- ✓ Damage to reputation and loss of business – if there is public distrust about how information is used.
- ✓ Compensation claims – if individuals are damaged by data losses

Compliance risks may include:-

- ✓ Non-compliance with the GDPR
- ✓ Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- ✓ Non-compliance with sector specific legislation or standards.

- ✓ Non-compliance with human rights legislation.

4. Identifying and evaluating privacy solutions

   a. Devise ways to reduce or eliminate privacy risks.
   b. Assess the costs and benefits of each approach, looking at the impact and the effect on the project outcomes.
   c. Keep it on the IG Risk Register until everyone is satisfied with the overall impact.

   This process should involve considering the aims of the project and the impact it will have. It also provides a record of the risks which the organisation has accepted as necessary for the project.

   Risk may be reduced by:-

   - ✓ Not collecting or keeping particular types of information.
   - ✓ Having retention periods which ensure information is only kept for as long as necessary and having planned secure destruction after that time.
   - ✓ Implementing appropriate technological security measures.
   - ✓ Training staff so they are aware of potential privacy risks.
   - ✓ Anonymising information where it is possible/appropriate
   - ✓ Providing staff with guidance on new systems and information sharing rules
   - ✓ Having systems which allow individuals to access their information more easily and make it simpler to respond to data subject access requests.
   - ✓ Ensuring individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
   - ✓ Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
   - ✓ Producing data sharing agreements that state what information will be shared, how it will be shared and who it will be shared with.

5. Signing off and recording the DPIA outcomes

   a. Obtain Exec level signoff
   b. Produce a DPIA report, based on the DPIA process conducted.
   c. Consider publishing the report or other relevant information, so it is available to appropriate stakeholders

6. Integrating the PIA outcomes back into the project plan

   a. Ensure that the action recommended by the DPIA is implemented and that this implementation is recorded.
   b. Continue to use the DPIA throughout the project lifecycle, when the project is reviewed or should it expand in the future.

GDPR related questions

1. Processed lawfully, fairly and in a transparent manner

- ✓ Have you identified the purpose of the project?
- ✓ How will individuals be told about the use of their personal data?
- ✓ Do you need to amend your privacy notices?
- ✓ Have you established which conditions for processing apply?
- ✓ If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
- ✓ Will the systems you are putting in place allow you to respond to subject access requests more easily?
- ✓ If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

   - ✓ Does your project plan cover all of the purposes for processing personal data?
   - ✓ Have potential new purposes been identified as the scope of the project expands?

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

   - ✓ Is the information you are using of good enough quality for the purposes it is used for?
   - ✓ Which personal data could you not use, without compromising the needs of the project?

4. Accurate and, where necessary, kept up to date

   - ✓ If you are procuring new software does it allow you to amend data when necessary?
   - ✓ How are you ensuring that personal data obtained from individuals or other organisations is accurate?

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

   - ✓ What retention periods are suitable for the personal data you will be processing?
   - ✓ Are you procuring software which will allow you to delete information in line with your retention periods?

6. Processed in a manner that ensures appropriate security of the personal data

   - ✓ Do any new systems provide protection against the security risks you have identified?

- ✓ What training and instructions are necessary to ensure that staff know how to operate a new system securely?
- ✓ Will the project require you to transfer data outside of the EEA?
- ✓ If you will be making transfers, how will you ensure that the data is adequately protected?

Human rights

If your organisation is subject to the Human Rights Act, you also need to consider:

- ✓ Will your actions interfere with the right to privacy under Article 8?
- ✓ Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need

DATA PROTECTION POLICY

This document details the data objects and items that are shared, and the use, storage, and security of the data that Schools share with EARL.

This agreement supports our joint obligation to comply not only with the Data Protection Act 2003 and the Information Commissioner's Office (ICO) mandate, but also the General Data Protection Regulations (GDPR) in force from May 2018.

All the personal data about school staff, parents or pupils held by The Data Processor has been supplied by the School. The School is the Controller of this data for the purpose of the GDPR and The Data Processor is acting merely as the agent of the School in applying this data for purposes approved by the School. It is therefore the responsibility of the School to ensure that this data is kept secure and accurate. The Data Processor will do whatever is necessary to ensure compliance with the letter and spirit of the regulations, as follows.

The principles which The Data Processor applies to the management of personal data are

1. That all The Data Processor data will be held only within the UK.
2. That all data will be encrypted during transmission and processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
3. That The Data Processor will only hold such personal data as is required to fulfil its obligations under this contract and that once this data is no longer required for this purpose, it will be deleted.
4. That The Data Processor will provide the School with whatever information it requires to fulfil its obligations in terms of data transparency.

5. In the event of any breach of the security of the personal data related to the School The Data Processor will inform the school within 48 hours so that the School may comply with its obligations to keep the affected people informed.

Signature of the The Data Processor Application form by authorised staff at any educational establishment within the UK indicates the acceptance by that entity of the terms of this agreement.

PERSONAL INFORMATION

Below is the list of personal information which The Data Processor requires to provide the The Data Processor service. Where appropriate, the data is classified in accordance with the UK Government's Information Security Design Manual Business Impact Levels.

1. PERSONAL INFORMATION ABOUT PUPILS WHO ARE CURRENTLY ON ROLL:

- Name, Gender, Age
- Assigned classes, clubs, groups, teams
- Unique Pupil Number
- All special needs flags and indicators
- Parental Consent

2. PERSONAL INFORMATION ABOUT STAFF CURRENTLY IN THE EMPLOYMENT OF THE SCHOOL:

- Name, Position
- Work email address
- Assigned classes, clubs, groups, teams

3. PERSONAL INFORMATION ABOUT PARENTS

- Name,
- Address (for product fulfilment only)
- Assigned children
- Email address
- Parent self-registrations are individually approved by the School.

4. INFORMATION ABOUT THE SCHOOL:

- Name, Address, Email address
- Name and contact details of the appointed
    - The Data Processor Administrators

- IT Managers
- Business Managers
- Accounts Managers.

INFORMATION MANAGEMENT

We do not collect or retain credit card information.

We do not sell any personal information to third parties. This information is only available to certain employees and contractors who have a need to it in the execution of their job.

We may use independent contractors to provide services on our behalf. Such third parties may have access to personal information in the course of providing services on our behalf. Any personal information that we provide to such third parties is protected under a confidentiality agreement. Such third parties will take commercially reasonable measures to keep your personal information safe, private and secure.

Payments made to The Data Processor for vouchers designed for use by others at a later date are held separate from the business funds of The Data Processor until the vouchers are cashed in order to pay for The Data Processor services. We automatically collect and store: the name of the domain and host from which you access the Internet;

- the Internet protocol (IP) address of the computer
- the date and time of access our sites
- the Internet address of the site from which the user arrived.

We use this information only as anonymous aggregate data to determine the number of visitors to different sections of our sites, to ensure the sites are working properly, and to help us make our sites more useful. We do not use it to track or record information about individuals.

When you use our services as a registered user, we utilize cookies to store information about your visits to make your revisits more efficient for you and us. It is necessary to place the cookie on your computer's hard drive in order for us to do this. We do not sell or give this information to any outside parties.

We use commercially reasonable measures to provide secure transmission of personal information to us. You should be aware that there is a level of risk involved in transmitting information over the Internet. As a result, we cannot ensure or warrant the security of the information that is transmitted over the Internet, and that you do so at your own risk.

Currently, The Data Processor does not work with third parties that provide advertisements to our site. This could change in the future, and if it does, a revised privacy policy will be issued.

Our website may contain links to other sites for your convenience. In most cases, those sites are not under our control, and they have their own policies regarding privacy, which you should review before using them. We bear no responsibility for linked websites and provide these links solely for your convenience and information.

DATA UPDATE AND SECURITY PROCESSES

It is the responsibility of the School to ensure that the data in The Data Processor is always current.

If the School cannot implement an automated update process it will assign a person to update data manually through the The Data Processor website or by sending and data revisions to The Data Processor customer services in the form of a spreadsheet,

To update data automatically, information is extracted from the school Management Information System (MIS) daily using Groupcall's industry leading and secure Xporter software. The data is securely uploaded to The Data Processor using industry standard SSL (secure socket layer) encryption. A unique identifier configured by EARL in Groupcall Xporter ensures that the information is linked to the correct customer account in The Data Processor. Groupcall Xporter accesses your school MIS system using credentials that you provide and cannot access it without them.

The information from the School is held inside the The Data Processor platform, which is hosted on dedicated servers based in England. You can find out more about the security and safety policies that affect your data by looking on the The Data Processor website or by contacting EARL.

The data held by The Data Processor is protected from exposure by multiple layers of firewalling, authentication, intrusion detection and physical access control.

DATA RETENTION

The Data Processor will delete all assessment data five years after the relevant school year-end. However, in order to fulfil its obligations under its contract with schools, The Data Processor will retain all media and associated metadata for five years after the last User tagged to that media has been Archived. Then it will be deleted.