Data Protection Impact Assessment (Evolve)

Summerhill School operates a cloud based system or 'hosted solution', called Evolve. Access to Evolve is through the internet. Resources are retrieved from Evolve via the Internet, through a web-based application, as opposed to a direct connection to a server at the school. Access to Evolve is through a web browser. As such Summerhill School must consider the privacy implications of such a system. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Summerhill School recognises that using a 'hosted solution' has a number of implications. Summerhill School recognises the need to have a good overview of its data information flow.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a cloud based system and the impact it may have on individual privacy.

The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. The location of the server is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the GDPR is satisfied by the school.

Summerhill School aims to undertake a review of this Data Protection Impact Assessment on an annual basis. A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce or eliminate the risks.
5. Sign off the outcomes of the DPIA.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
What is the aim of the project? – Evolve is a software system which provides an online platform for the following modular systems: Evolvevisits; Evolveaccidentbook; Evolveclubs; and Evolve+. Summerhill School uses: EVOLVE *visits* is an online system for the planning, approval and management of educational visits, sports fixtures and extra-curricular activities. It reduces paperwork, simplifies procedures, produces self-review and inspection preparation data, and improves staff confidence in that they automatically follow both employer, and National Guidelines. Evolve will be for internal use only and there will be no sharing of information with outside agencies. Information will be shared only as appropriate with parents, teachers and teaching assistants. In terms of reporting accidents and incidents it may be necessary to share information with external agencies such as the Department for Education, Health and Safety Executive, Local Authority, etc. The lawful basis for sharing this information in contained in the schools Privacy Notices (Pupil), (Workforce), and (Governors and Volunteers). Evolve is a hosted system which means that all updates, maintenance and management can be performed in a central location by eduFOCUS Ltd *(the owners of Evolve)*. The platform enables Summerhill School to improve their management of educational visits, sports fixtures and extra-curricular activities, management of staff, Summerhill School and visitor injuries, illnesses and accidents, and planning, providing and managing school extra-curricular clubs and activities, whilst reducing staff time, paperwork and administration. The platform enables Summerhill School to centralise the data, share information with parents and other relevant agencies when and where appropriate. Summerhill School will undertake the following processes: 1. Collecting personal data

2. Recording and organising personal data
3. Storing personal data
4. Copying personal data
5. Retrieving personal data
6. Deleting personal data

By opting for Evolve the school aims to achieve the following:

1. Management of pupil/workforce/volunteer information in one place
2. Security and integrity of data
3. Storage of information electronically rather than manually
4. Portal for recording information
5. Providing bespoke reports for difference audiences, e.g. Parents or agencies
6. Identifying trends and patterns
7. Secure access across all devices wherever the setting

Cloud based systems enable the school to upload documents and other files to a hosted site to share with others within school. These files can then be accessed securely from a PC in the school.

eduFOCUS Ltd cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated accordingly.

The school is the data controller and eduFOCUS Ltd is the data processor.

Summerhill School has included Evolve within its Information Asset Register.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The Privacy Notices (student) for the school provides the legitimate basis of why the school collects pupil data. Specifically this relates to health and safety and safeguarding of vulnerable groups. Evolve will be specifically referenced in the school's Privacy Notice (student).

How will you collect, use, store and delete data? – Evolve may collect information from pupil records, Special Educational Needs (SEN) records, Education Health Care Plans (EHCP). If personal data concerning health is included it is considered under data protection law as special category data. Evolve can upload pupil data from the schools Management Information System which is then uploaded via a secure transfer method to the platform's portal. The information will be stored in the platform. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – Personal data may come from the following sources: safeguarding records, SENCO records, Education Health and Care Plans, Pupil Records, and Common Assessment Framework.

Will you be sharing data with anyone? – Summerhill School routinely shares pupil information with relevant staff within the school, schools that the pupil attends after leaving, the Local Authority, the Department for Education, Health Services, the schools Management Information System and various third parties as appropriate. This may include Governors, Health and Safety Executive, local authority professionals, and Ofsted.

However, this does not mean that Summerhill School shares Evolve access to the third parties.

What types of processing identified as likely high risk are involved? – The information is transferred securely from the school to the server, which is hosted remotely on a server within the United Kingdom. Access to information on Evolve is controlled through passwords and access controls.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
What is the nature of the data? – Personal data may relate to the following categories: *Student data* relates to management information system unique number (UPN), forename, surname, date of birth, pupil home address, ethnicity, first language and gender of the child. This may also include group identification such as Class, Registration Group and Year Group. Pupil premium indicator, in LEA care, Special Educational Need, eligibility for free school meals, dietary needs, medical conditions with notes, passport number (if applicable regarding visits), and trip notes. *Parent data* including e-mail and telephone contact, relationship of the contact. *Staff data* relates to forename, surname, date of birth, work e-mail and telephone contact. Staff code and gender. **Special Category data?** – Data revealing medical details is collected by the school and contained in Evolve. The lawful basis for collecting this information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.* **How much data is collected and used and how often?** – Personal details relating to pupils are obtained from parent/pupil information systems. Additional content may be obtained from classroom/teacher observation/agency partners. EduFocus Ltd will only collect and process data, including special category data, on behalf of the school that is necessary for the performance of Evolve. Special category may be entered directly into Evolve by the school or it may be electronically transferred into Evolve. **How long will you keep the data for?** – The school follows the good practice in terms of data retention as set out in the IRMS Information Management Toolkit for Schools and also as set out within the school's data retention policy. **Scope of data obtained?** – The scope of data obtained by schools will include the following: name of pupil, date of birth, age, gender, home address, phone number, e-mail address, location data, online identifier, UPN, SEN, first language, photograph of the pupil (management information system), year group, registration group/class/house/division, contact details for the pupil's home address and mobile number, names and contact details

for parents/guardians, database IDs for siblings within the same school, flags to indicate whether the pupil is disabled, medical condition, pupil premium, free school meals, and in care flags. Behaviour. Racial and ethnic origin. Religious belief. Physical or mental health or condition, biometric or genetic data.

Not all of this data will be required on the Evolve platform.

The geographical area covered is from Year 7 to Year 11 students.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

What is the nature of your relationship with the individuals? – Summerhill School collects and processes personal data relating to its pupils to ensure the school provides education to its Summerhill Schools with teaching staff delivering the National Curriculum.

Through the Privacy Notice (Student) Summerhill School is committed to being transparent about how it collects and uses data and to meeting its data protection obligation.

How much control will they have? – Not all staff will have access to information held on Evolve. Access can be restricted so that only designated staff can see information that is relevant to them. Access to the data held on Evolve will be controlled by username and password. The platform will be used internally only from devices based within the school. Access to the platform can be revoked at any time.

Do they include children or other vulnerable groups? – All of the data will relate to children.

Are there prior concerns over this type of processing or security flaws? – How is the information stored? Does the cloud provider store the information in an encrypted format? What is the method of file transfer? How secure is the network and what security measures are in place?

Summerhill School recognises that moving from a manual system to an electronic system which holds sensitive personal data in the cloud raises a number of General Data Protection Regulations issues as follows:

- **ISSUE:** Evolve will be storing personal data

RISK: There is a risk of unauthorized access to information by third parties
MITIGATING ACTION: eduFOCUS Ltd offers the following in terms of security: (1) scripted in Active Server Pages, and all dynamic data is stored a SQL database environment; (2) automatic log-out after 20 minutes of inactivity (configurable); (3) secure password protected web service; (4) users can be disabled to prevent access, but their visit history maintained; and (5) eduFOCUS Ltd have installed advanced firewalls, enterprise-level virus protection on all servers

eduFOCUS Ltd have invested in additional data centre security features to help ensure protection of data, including DDoS security feature, Web Application Firewalls (WAFs)(managed CISCO firewall protection), Proactive Threat Monitoring and Threat Response. Further information is available in 'EVOLVE Technical & Security Measures' in Resources.

UK based data centre offers 24/7/365 onsite technical support to respond quickly to hardware issues, aggregated direct connections to the internet backbone to provide reliable and expandable bandwidth and a sophisticated "no single point of failure" system to ensure maximum connectivity.

CCTV monitoring, motion detection, 24/7/365 security guards and an advanced access control system are also in-situ.

- **ISSUE**: Transfer of data between the school and the cloud.
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: Data transferred between server and browser is encrypted using TLS protocol

- **ISSUE:** Use of third party sub processors?
  RISK: Non compliance with the requirements under GDPR
  MITIGATING ACTION: eduFOCUS Ltd will only use the services of third parties for its own organisational purposes and not to use the services to provide services to third parties.

  eduFOCUS Ltd will process the school's personal data only on documented written instructions from the school, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by applicable law to which EduFocus Ltd is subject and in such a case eduFOCUS Ltd will inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?

RISK: The potential of information leakage
MITIGATING ACTION: eduFOCUS Ltd server infrastructure is housed in one of the UK's leading data centres. Evolve is a fully hosted service solution - clients do not require any additional hardware or software in order to use or manage the service. It is scripted in Microsoft Active Server Pages, is hosted on the Microsoft Windows Server 2012 R2 platform and stores dynamic data within a clustered SQL database environment

ISSUE: Cloud solution and the geographical location of where the data is stored
RISK: Within the EU, the physical location of the cloud is a decisive factor to determine which privacy rules apply. However, in other areas other regulations may apply which may not be Data Protection Law compliant
MITIGATING ACTION: In operating the Evolve website it will only transfer data that is collected from the data controller to secure data centres in the EEA for processing and storing

eduFOCUS Ltd will not transfer any personal data outside of the European Economic Area without the Customer's prior written consent.

- **ISSUE:** The right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object
  RISK: The school is unable to exercise the rights of the individual
  MITIGATING ACTION: Staff can access their data via their Evolve account (if applicable). Parents and students can access their data via their 'my Evolve' account (if applicable). For data subjects that do not have user accounts in Evolve they can make Subject Access Requests to the data controller (the school)

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: GDPR non-compliance
  MITIGATING ACTION: eduFOCUS Ltd have introduced new features to allow authorised users to hard delete data so that data controllers can comply with their obligations to destroy data where there is no longer a justifiable reason to retain the data

- **ISSUE:** Responding to a data breach
  RISK: GDPR non-compliance
  MITIGATING ACTION: All eduFOCUS Ltd staff have undertaken GDPR training on data management and security. All eduFOCUS Ltd staff are aware of the incident response procedures. eduFOCUS Ltd continue to conduct comprehensive ongoing security risk assessments. Security is a top priority for eduFOCUS Ltd, and additional training and security measures builds on the robust protocols that already exist to prevent and respond to data breaches and vulnerabilities

- **ISSUE:** Data is not backed up
  RISK: GDPR non-compliance
  MITIGATING ACTION: eduFOCUS Ltd back up all customer data held on such servers no less than once in any 24-hour period.

- **ISSUE:** No deal Brexit
  RISK: GDPR non-compliance
  MITIGATING ACTION: Evolve is fully hosted by eduFOCUS Ltd in a UK based data centre

- **ISSUE:** Subject Access Requests
  RISK: The school must be able to retrieve the data in a structured format to provide the information to the data subject
  MITIGATING ACTION: Staff can access their data via their Evolve account (if applicable). Parents and pupils can access their data via their 'my Evolve' account (if applicable). For data subjects that do not have user accounts in Evolve they can make Subject Access Requests to the data controller (the school)

- **ISSUE:** Data Ownership
  RISK: GDPR non-compliance
  MITIGATING ACTION: As Data Controller the school maintains ownership of the data. eduFOCUS Ltd is the data processor.

  As data processor, eduFOCUS Ltd will only process personal data on the instructions from the data controller (the school) and its nominated authorised user(s).

  As data processor eduFOCUS Ltd will comply with security obligations equivalent to those imposed on the data controller itself

- **ISSUE:** Cloud Architecture
  RISK: The school needs to familiarise itself with the underlying technologies the cloud provider uses and the implications these technologies have on security safeguards and protection of the personal data stored in the cloud
  MITIGATING ACTION: EVOLVE is hosted on state of the art servers in the UK

  eduFOCUS Ltd have introduced a new EVOLVE Data Security Dashboard which allows System Administrators to configure and implement additional security features including Two-Factor Authentication, Email Single Sign-On (ESSO), Password Expiry Periods, Password Reuse Rules, Password Fail Rules, Session Time-out Periods and a list of all users that have System Administrator permissions

- **ISSUE:** GDPR Training
  RISK: GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Evolve

- **ISSUE:** Security of Privacy
  RISK: GDPR non-compliance
  MITIGATING ACTION: Accreditations include: ISO9001:2008, ISO14001:2015, Cyber Essentials, G-Cloud 9, PAS2060, PCI DSS Compliance. In addition to these accreditations eduFOCUS Ltd has attained:

  ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. Microsoft has earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure

  ISO 27018: is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Microsoft has been certified compliant with ISO 27018 for its shared Common Infrastructure

  eduFOCUS Ltd is registered with the Information Commissioners Office under reference Z9779026

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The school moving to a cloud-based solution will realise the following benefits:

1. Management of pupil/workforce/volunteer information in one place
2. Security and integrity of data
3. Storage of information electronically rather than manually
4. Portal for recording information
5. Providing bespoke reports for difference audiences, e.g. Parents or agencies
6. Identifying trends and patterns
7. Secure access across all devices wherever the setting

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
Evolve is already established in Summerhill School. The view of YourIG has also been engaged to ensure Data Protection Law compliance

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil). The lawful basis includes the following: ▪ Health and Safety at Work Act ▪ Keeping Children Safe in Education ▪ Safeguarding Vulnerable Groups Act ▪ Working together to Safeguard Children Guidelines (DfE) The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law Evolve will enable the school to uphold the rights of the data subject; the right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making; these rights will be exercised according to safeguarding considerations. The school will continue to be compliant with its Data Protection Policy.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Data transfer; data could be compromised	Possible	Severe	Medium
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Upholding rights of data subject	Probable	Significant	Medium
Data Retention	Probable	Significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Data Transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection & resilience	Data Centre based in the UK	Reduced	Medium	Yes
Data Breaches	Documented in contract and owned by school	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Upholding rights of data subject	Technical capability to satisfy rights of data subject	Reduced	Low	Yes
Data Retention	Implementing school data retention periods as outlined in the IRMS Information Management Toolkit for Schools	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	**[Insert name]**	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	**[Insert name]**	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Technical recommendations to be clarified with third party as follows: *(1) How is the information stored on the server? (e.g. is the server shared with other schools, what security is in place to maintain the integrity of the school's data?)* *(2) Where is the server located?* *(3) Is personal data stored in an encrypted format? (if not how is the information stored?)* *(4) What is the method of file transfer from school to the remote server and vice versa? (is it via a secure network?)* *(5) How secure is the network? (The school wishes to mitigate against the risk of compromise or unlawful access when personal data is transferred)security* *(6) What mitigating actions are put in place when appointing third party sub contractors* *(7) What security measures are in place? (firewalls, etc?)* *(8) How and when is data backed up?* *(9) Confirmation that personal data relating to Evolve is kept on servers located in the UK including backup servers?*		
DPO advice accepted or overruled by:	No	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	**[Insert name]**	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	**[Insert name]**	The DPO should also review ongoing compliance with DPIA