Data Protection Impact Assessment (Canva)

The Earls High School operates a cloud based system. As such The Earls High 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.

The Earls High School recognises that moving to a cloud service provider has a number of implications. The Earls High 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 cloud 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 UK GDPR is satisfied by the school.

The Earls High School aims to undertake 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.

Contents

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? – Canva operates an online design platform and media licensing service that enables users, members, artists, designers, photographers and others to design and collaborate. Canva provide ready-made media and content that is licensable for use in accordance with Canva's various licenses.

The Earls High School will undertake the following processes:

1. Collecting personal data
2. Recording and organizing personal data
3. Structuring and storing personal data
4. Copying personal data
5. Retrieving personal data
6. Deleting personal data

By opting for an internal server based solution the school aims to achieve the following:

1. Scalability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time
7. Good working practice, i.e. secure access to sensitive files

Canva for Education (and all content and media incorporated therein) for educational purposes may be used by schools. In the context of schools this can include using Canva as a platform to produce promotional material, newsletters, school memorabilia for school proms, leavers books, etc.

The Earls High School uses Canva for Education. Canva provide this service to Teachers at a Qualified Educational Institution and only where proof is provided.

Students may only be invited to Canva for Education only by a Teacher and shall be eligible to hold a Canva for Education account for so long as they are a student at a Qualified Educational Institution and use Canva under the supervision of a Teacher.

"Qualified Educational Institution" means a public or private primary or secondary school that has been accredited by the Department for Education and has the primary purpose of teaching its enrolled students.

The cloud service provider cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated especially with reference to the storing of pupil and workforce data in the cloud.

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 (pupil) for the school provides the legitimate basis of why the school collects data. The lawful basis in order to process personal data in line with the 'lawfulness, fairness and transparency principle is as follows:

6.1 (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; e.g. health & safety and safeguarding
6.1 (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
6.1 (f) Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

The school has considered the lawful basis by which it processes personal data. This is recorded in The Earls High School Privacy Notice (Pupil).

How will you collect, use, store and delete data? – The information collected by the school is retained on Canva.

Some of the personal data collected falls under the UK GDPR special category data. For example, the use of photographs of pupils when uploaded to the Canva platform may identify their ethnicity or racial origin.

Canva may ask for certain information when the school registers for a Canva account or corresponds with Canva (such as a username, your first and last names, birthdate, phone number, profession, and e-mail address).

If the school joins the Canva forum located at http://community.canva.com where users discuss Canva's services and products (Community), Canva will receive additional information (such as school location, name, website and social media links, personal description) which will be associated with school posts and activity in the Community.

Canva also collect any messages sent by the school, and may collect information the school provides in user content posted to the Service (such as text and photos the school uploads to use in school designs or posts in the Canva Community). Canva use this information to operate, maintain, and provide the features and functionality of the Service to the school, to correspond with the school, and to address any issues the school raises about the Service.

The information is retained in accordance with the school's Data Retention Policy.
What is the source of the data? – Routinely pupil information is collected via registration forms when pupils join the school, pupil update forms the school issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools.

Workforce information is collected through application forms, CVs or resumes; information obtained from identity documents, forms completed at the start of employment, correspondence, interviews, meetings and assessments.

The Earls High School recognize the importance of GDPR principle of Article 5 1 (c) "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (the principle of data minimisation).

The data provided to Canva will be restricted to the first name of the student, their photograph, accompanied by the name of the school only. The data will relate to Year 6 pupils only. Additional data may include the name of the teacher, name of school, and e-mail address.

Will you be sharing data with anyone? – The Earls High School may share pupil, workforce and visitor information with relevant staff within the school, the Local Authority, the Department for Education, Health and Safety Executive (HSE), Health Services, and Canva.

The Earls High School may share workforce information internally with people responsible for HR, senior staff, Health and Safety Executive (HSE), Health Services, with the Local Authority, and the Department for Education.

In terms of sharing data with Canva The Earls High School will apply the GDPR principle of Article 5 1 (c) "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (the principle of data minimisation).

What types of processing identified as likely high risk are involved? – Some of the personal data collected falls under the UK GDPR special category data. For example, the use of photographs of pupils when uploaded to the Canva platform may identify their racial origin or ethnicity.

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law in respect to* The Children Act and subsequent amendments and The Education Act. The lawful basis is also covered by Schedule 1, part 2, paragraph 8 (Substantial Public Interest Conditions - equality of opportunity or treatment). This is further documented in the school's Privacy Notice.

However, in terms of The Earls High School using Canva to upload the name and photograph of the pupil to its platform the school will be using consent as its lawful basis.

The WAN link from the school is a dedicated lease line so is not shared with other users like domestic broadband users, therefore it is protected from interception.

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? – Pupil data relates to personal identifiers and contacts (such as name of the pupil). Characteristics (such as age, gender, racial origin and ethnic group).

Workforce data relates to personal information (such as name and contact details, employee or teacher number). Special categories of data (such as racial origin and ethnic group).

Special Category data? – Some of the personal data collected falls under the UK GDPR special category data. For example, the use of photographs of pupils when uploaded to the Canva platform may identify their racial origin or ethnicity.

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law in respect to* The Children Act and subsequent amendments and The Education Act. The lawful basis is also covered by Schedule 1, part 2, paragraph 8 (Substantial Public Interest Conditions - equality of opportunity or treatment). This is further documented in the school's Privacy Notice.

How much data is collected and used and how often? – The data provided to Canva will be restricted to the first name of the student, their photograph, accompanied by the name of the school only. The data will relate to Year 6 pupils only.

In terms of sharing data with Canva The Earls High School will apply the GDPR principle of Article 5 1 (c) "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (the principle of data minimisation).

How long will you keep the data for? – Consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools and the School's Data Retention Policy.

Scope of data obtained? – How many individuals are affected (pupils, workforce, governors, and volunteers)? And what is the geographical area covered?

Year 7 to 11 pupils 1600 and workforce 130

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)?

The school provides education to its students with staff delivering the National Curriculum

What is the nature of your relationship with the individuals? – The Earls High School collects and processes personal data relating to its pupils and employees to manage the parent/pupil and employment relationship.

Through the Privacy Notice (pupil/workforce) The Earls High 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? – Access to the files will be controlled by username and password. Canva is hosting the data and has the ability to access data on instruction of The Earls High School who is the data controller for the provision of supporting the service.

The school will be able to upload personal data from its PC via a web browser for the data to be stored remotely by the service provider.

Do they include children or other vulnerable groups? – Canva will include the following: the first name of the student, their photograph, accompanied by the name of the school only. The data will relate to Year 6 pupils only.

Are there prior concerns over this type of processing or security flaws? – Canva have ISO 27001 accreditation, which is the international standard for information security management.

The Earls High School recognises a number of UK General Data Protection Regulations issues as follows:

- **ISSUE:** The cloud based solution will be storing personal data including sensitive information
  RISK: There is a risk of uncontrolled distribution of information to third parties
  MITIGATING ACTION: Employees of Canva can only access the data they need to do their job and Canva store personal data and designs with cloud providers who have top-tier physical security controls

  Canva's threat detection, logging and alerting systems notify their oncall teams about potential incidents. Canva peer review and test their code prior to release, including manual and automated checks for security issues

  Canva's security team is comprised of dedicated Security Engineers who work across the company to ensure our product, platforms and operations are secure

  ISO 27001 certification requires Canva to have periodic external audits of our information security management system and security controls

- **ISSUE**: Transfer of data between the school and the cloud
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: Canva keep personal data and designs secure in transit and at rest. In transit, personal data and designs are only accessible via TLS/SSL, and at rest, designs are encrypted with AES256

- **ISSUE:** Use of third party sub processors?
  RISK: Non-compliance with the requirements under UK GDPR
  MITIGATING ACTION: Canva share school information with third-party service providers for the purpose of providing the Service to the school and to facilitate Canva's legitimate interests in providing a service which is useful and safe to the school. Those service providers will only be provided with access to school information as is reasonably necessary for the purpose that Canva has engaged the service provider, and Canva will require that such third parties comply with their Privacy Policy, appropriate data processing terms and any applicable laws

We may also share data with the data subject at the request of this individual in compliance with a Subject Access Request
Canva may share data with a third party if legally required to do so

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: By default, all content the school posts on Canva is private

  Personal data is stored in systems that are only accessible via the Canva application. When a school logs in to Canva, they give the school's Canva account access to the private files. Personal data can only be accessed by logging in to the school account. The school's personal data cannot be accessed by anyone that is not logged in to Canva, or anyone using a different account unless the school shares its personal data

  Canva employs specialist external services and tools to conduct multiple different types of security assessments

  Canva also run weekly vulnerability scans against its production environments, and engage external penetration testers to conduct multiple penetration tests throughout the year

- **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: All student data remains hosted in AWS in the United States. Canva have standard contractual clauses in place with all sub processors (below) to ensure compliance with Article 46 of the GDPR. These include Atlas (data storage), Amazon Web Services (data storage), Appbot (user support), Braze (Marketing to teachers (not students)), Concentrix (user support), Jira (user support), Loggly (logging), Looker (Analysis of aggregated user behaviour data), Mailchimp (service emails), Mode

(Analysis of aggregated user behaviour data), Sentry (error monitoring), Snowflake (data storage), Usersnap (user support) and Zendesk (user support)

Where Canva transfer school information to a third party provider that is not located in the EEA, and is not subject to an adequacy decision by the EU Commission, Canva will require those third party providers to enter into an agreement that provides appropriate safeguards for school information, including by using the EU Model Clauses

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Access to schools' data is strictly controlled and monitored at Canva, and they employ a 'least privilege' code of practice within the organisation

  Personal data is stored in systems that are only accessible via the Canva application. When a school logs in to Canva, they give the school's Canva account access to the private files. Personal data can only be accessed by logging in to the school account. The school's personal data cannot be accessed by anyone that is not logged in to Canva, or anyone using a different account unless the school shares its personal data

- **ISSUE:** Data is not backed up
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: All data is back up in line with the requirements as documented under ISO 27001

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Canva is fully compliant with UK GDPR data security handling and reporting. Canva's threat detection, logging and alerting systems notify their oncall teams about potential incidents

- **ISSUE:** Data Retention
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: If a student account is inactive for more than 12 months, Canva will send an email to the email address associated with that account to confirm if the

student wishes to continue using the service. If the student does not respond within 3 months of receipt of that email and there has been no activity on the account, Canva will delete their account

Upon termination of a school's Canva for Education account, Canva will delete all student accounts associated with that school

Under the Canva Terms and Conditions once the account is closed the posts and other information will remain in an anonymized form. To request removal of school information from Canva the school can contact, please privacy@canva.com. If Canva are unable to remove any of the school's information, they will let the school know why

- **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: Canva has the functionality to respond to Subject Access Requests. Canva agrees to comply with Subject Access Requests relating to the data it stores

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school remains the data controller. Canva is the data processor

- **ISSUE:** Post Brexit
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Where Canva transfer school information to a third party provider that is not located in the EEA, and is not subject to an adequacy decision by the EU Commission, Canva will require those third party providers to enter into an agreement that provides appropriate safeguards for school information, including by using the EU Model Clauses

- **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: Canva stores its data in the cloud using several types of storage, depending on the type of data, including databases, file storage and other systems

Canva systems are only accessible by people and services who need access

Canva encrypt designs using AES256. This means that personal data and designs are unreadable by someone with access to the disks holding the personal data and designs

- **ISSUE:** Third-party Access to Data
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Before any access is granted to the school's data held in Canva, to third-party applications, the school must give explicit authorization and review the type of data that the application is requesting. The permissions can be revoked at any time by the school

- **ISSUE:** UK GDPR Training
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Canva in strict compliance with ISO 27001 and agree to abide by the Canva data sharing and confidentiality policies

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Canva is ISO 27001 certified. This certification means that, as an organisation, Canva have the people, processes and systems in place to effectively identify, assess, treat and monitor our information security risks. It means that Canva aim to have security built into every facet of its operations, and that they strive to improve there security posture through a process of continuous improvement

  ISO 27001: is one of the most widely recognized, internationally accepted independent security standards

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 processing of this data will allow the school to function safely. We know where our students are at any time and can access the vital information we need to keep them safe. We can build up patterns of academic achievement and attitude so that we can best support our students.

Combined staff and student data allows for timetable creation and school organisation with registers.

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?

As the system is already in use there is no need to consult stakeholders. Should systems change we would consult more stakeholders.

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 and Workforce). The lawful basis includes the following:

- Childcare Act 2006 (Section 40 (2)(a)
- The Education Reform Act 1988
- Further and Higher Education Act 1992,
- Education Act 1994; 1998; 2002; 2005; 2011
- Health and Safety at Work Act
- 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. The cloud based solution 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?

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
Data Breaches	Possible	Significant	Medium
Post Brexit (GDPR noncompliance)	Possible	Significant	Medium
Subject Access Request	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
Data Breaches	Documented in contract and owned by school	Reduced	Low	Yes
Post Brexit	Standard Contractual Clauses in place	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Implementing school data retention periods in the cloud	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Jamie Fox	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Jamie Fox	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 *(the following questions were asked of the third party by the school's Data Protection Officer)*:

1. The Privacy Notice mentions that schools data may be transferred to the US, Australia, Europe and anywhere else the service is operated.

   Given post Brexit where would the school's data be hosted and what safeguards are in place?

2. We understand following termination or deactivation of a User account, Canva will retain profile information and User Content for a commercially reasonable time, and for as long as Canva have a valid purpose to do so. In particular, Canva will retain third party information for the purpose of complying with its legal and audit obligations, and for backup and archival purposes.

   In practice how long would you keep school data such as photos of children for?

DPO advice accepted or overruled by: n/a

If overruled, you must explain your reasons

Comments:

n/a

Consultation responses reviewed by:

Anna Wade If your decision departs from individuals' views, you must explain your reasons		
Comments: [Comments provided]		
This DPIA will kept under review by:	Anna Wade	The DPO should also review ongoing compliance with DPIA