Data Protection Impact Assessment (ClassDojo)

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server at the school. Greenfield Primary School operates a cloud based system or hosted solution called ClassDojo. Access to Class Dojo is through a web browser. As such Greenfield Primary 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. Greenfield Primary School recognises that moving to a cloud service provider has a number of implications. Greenfield Primary 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 GDPR is satisfied by the school.

Greenfield Primary 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.

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? – ClassDojo is a communication platform which assists teachers to encourage pupils in class and engage with parents. In the classroom setting teachers can use ClassDojo to give students encouragement or "feedback points". Teachers can also post assignments for pupils to complete on ClassDojo ("Activities"). If using ClassDojo apps or the ClassDojo platform it is possible to sync them with each other. Outside the classroom setting, teachers may use ClassDojo to engage families and parents. ClassDojo can be used to instantly message parents with text messages, pictures, videos and stickers, and also add posts to Class Story and School Story apps on the Class Dojo platform. It connects teachers, parents, and students who use it to share photos, videos, and messages through the school day. Schools use ClassDojo to work together as a team, share in the classroom experience, and bring big ideas to life in their classrooms and homes. Parents access and set up an account on ClassDojo using a unique parent code provided by their child's teacher or through an e-mail/SMS invitation, or by choosing their child's teacher from within the list shown within ClassDojo App or ClassDojo Website. An account for a pupil can be set up by: (1) an account being created at school by the teacher; (2) receive a unique code from their teacher to create their own account with a username and password; or (3) have their parents create their own student account at home. ClassDojo is a hosted system which means that all updates, maintenance and management can be performed in a central location by ClassDojo. ClassDojo will help deliver a cost effective solution to meet the needs of the business. The cloud based system will improve accessibility and ensure information security.

Greenfield Primary 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 a cloud based solution the school aims to achieve the following:

1. Scaleability
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

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.

ClassDojo 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 ClassDojo is the data processor.

Greenfield Primary School has included ClassDojo within its Information Asset Register.

Cloud based systems enable the school to upload documents, photos, videos, and other files to a website to share with others or to act as a backup copy. These files can then be accessed from any location or any type of device (laptop, mobile phone, tablet, etc).

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 lawful basis of why the school collects data. Specifically under GDPR Article 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.'

How will you collect, use, store and delete data? – The information is obtained when setting up an account. Typically this will include the name of the parent/guardian, mobile telephone number and e-mail address. For the pupil it will include their first and last name and date of birth.

Class Dojo collects the minimal amount of information from pupils necessary to register for an account. The pupil account, profile, or portfolio is never made available or visible to the public through ClassDojo.

ClassDojo will only be kept for as long as the pupil account is active. If a pupil's account is inactive for twelve months or more ClassDojo will automatically delete the pupil account.

ClassDojo also apply a one year deletion policy for feedback points on an ongoing basis. Teachers can delete feedback points at any time. The school's Data Retention Policy will be amended to reflect this.

What is the source of the data? – To create a ClassDojo account either as a teacher, a member of SLT, or parent/guardian the following personal data will be required: first and last name, e-mail address, mobile telephone number, password and a profile photograph.

If the teacher is creating the pupil account they will provide the pupil's first and last name and their class. If the parent is creating the account they will provide the pupil's first and last name. The teacher may also provide a photograph of themselves. Good practice would encourage the school as data controller to obtain photo consent.

The school may provide geolocation information to help ClassDojo identify the school and other schools.

Will you be sharing data with anyone? – Greenfield Primary School Access is restricted to a private feed of moments from the classroom and school that only students, parents, teachers, and SLT can see. ClassDojo has the functionality to share information through the

service with other ClassDojo teachers, school leaders, students or parents. This can include account information, feedback points awarded to students (that teachers or school leaders teach) or to their child (if they are a parent) or other information you share through ClassDojo Messaging, Class Story, School Story or the other collaboration tools. Sharing this information is voluntary and the users should bear in mind that any information shared in this way, can be stored by others.

What types of processing identified as likely high risk are involved? – Transferring 'special category' data from the school to the cloud. Storage of personal and 'special category data in the Cloud.

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 information includes first and last name of pupil and their class/year. Parent/guardian information required includes first and last name, e-mail address, telephone number, password and a profile photograph. To create a ClassDojo account as a teacher or school leader information required includes first and last name, e-mail address, telephone number, password and a profile photograph. **Special Category data?** –GDPR special category data includes race; ethic origin; religion; biometrics; and health. No special category data is used in this setting. **How much data is collected and used and how often?** – Personal data is collected for all pupils. Additionally personal data is also held respecting the school's workforce, Board of Governors, Volunteers, and Contractors. Data relating to sports coaches and other educational specialist is contained within the Single Central Record to ensure health and safety and safeguarding within the school. **How long will you keep the data for?** – Consider the data retention period as outlined in the IRMS Information Management Toolkit for Schools **Scope of data obtained?** – How many individuals are affected (pupils, workforce)? And what is the geographical area covered? EYFS, Year 1 to Year 6 pupils 280, and workforce 41.

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?** – Greenfield Primary School collects and processes personal data relating to its pupils and employees to manage the parent/pupil and school relationship. Through the Privacy Notice (pupil/workforce) Greenfield Primary 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. Cloud Service provider is hosting the data and will not be accessing it. The school will be able to upload personal data from its PC for the data to be stored remotely by a service provider. Any changes made to files are automatically copied across and immediately accessible from other devices the school may have. **Do they include children or other vulnerable groups?** – Data will be collected for EYFS and Year 1 to Year 6 pupils at Greenfield Primary School. The cloud service provider will provide access controls to the files. For example, files designated as private – only the school can access the files; public – everyone can view the files without any restriction; and shared – only people the school invite can view the files. **Are there prior concerns over this type of processing or security flaws? –** Does the cloud provider store the information in an encrypted format? What is the method of file transfer? For example, the most secure way to transfer is to encrypt the data before it leaves the computer. Encryption does have its limitations inasmuch as the encryption key will need to be shared with others to access the data.

Greenfield Primary School recognises that moving to a cloud based solution raises a number of 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: ClassDojo perform application security testing, penetration testing; conduct risk assessments; and monitor compliance with security policies. ClassDojo periodically reviews its information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.

- **ISSUE**: Transfer of data between the school and the cloud.
  RISK: Risk of compromise and unlawful access when personal data is transferred.
  MITIGATING ACTION: ClassDojo encrypts the transmission of personal data using secure socket layer technology (SSL/TLS) by default. ClassDojo ensure passwords are stored and transferred securely using encryption and salted hashing.

- **ISSUE:** Understanding the cloud based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage.
  MITIGATING ACTION: Personal data is stored on a server equipped with industry standard firewalls. In addition, the hosting facility provides a 24 x 7 security system, video surveillance, intrusion detection systems and locked cage areas. ClassDojo's database where personal data is stored is encrypted at rest, which converts all personal data stored in the database to an unintelligible form.

- **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: ClassDojo is hosted in the United States. Where ClassDojo transfer, store and process personal data outside of the European Union it has ensured that appropriate safeguards are in place to ensure an adequate level of protection for the rights of the data subject based on the adequacy of the receiving country's data protection laws or EU-US Privacy Shield principles.

  The Privacy Shield provides many important benefits to U.S.-based organizations, as well as their partners in Europe. These include: (1) Participating organizations are deemed to provide "adequate" privacy protection, a requirement (subject to limited derogations) for the transfer of personal data outside of the European Union under the EU General Data Protection Regulation (GDPR) on Data Protection; (2) EU Member State requirements for prior approval of data transfers either are waived or approval will be

automatically granted; and (3) Compliance requirements are clearly laid out and cost-effective.

ClassDojo complies with the Privacy Shield Principles for all onward transfers of personal data from the EU, including onward transfer liability provisions.

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: ClassDojo recognizes the rights of data subjects and the right of the data controller to limit the ways ClassDojo uses the school's personal information. Privacy Shield principles recognizes data subject rights to obtain confirmation of whether ClassDojo has data about them and the right to correct, amend, and delete if inaccurate.

- **ISSUE:** Implementing data retention effectively in the cloud.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: ClassDojo will only be kept for as long as the pupil account is active. If a pupil's account is inactive for twelve months or more ClassDojo will automatically delete the pupil account. ClassDojo also apply a one year deletion policy for feedback points on an ongoing basis. Teachers can delete feedback points at any time. The school's Data Retention Policy will be amended to reflect this. The Privacy Shield recognizes the principle of data minimization and the need to retain information only for as long as it serves a processing purpose.

  School to take into consideration backups and if the data is stored in multiple locations and the ability to remove the data in its entirety.

- **ISSUE:** Responding to a data breach.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: The Privacy Shield recommends that reasonable precautions are taken to protect from loss, misuse, unauthorised access, disclosure, alteration, and destruction of personal data. The school recognizes the need to define in their contract a breach event and procedures for notifying the school and the school managing it.

- **ISSUE:** Transfer of personal data outside the EEA.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: ClassDojo may work with service providers located outside the EEA. ClassDojo is certified under the EU-US Privacy Shield Framework; and/or the existence of any other specifically approved safeguard for data transfers as recognised under EU Data Protection Laws.

- **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: ClassDojo has the technical capability to ensure the school can comply with a data subject access requests. Privacy Shield principles recognizes data subject rights to obtain confirmation of whether ClassDojo has data about them and the right to correct, amend, and delete if inaccurate. This may be included as part of the contract.

- **ISSUE:** Data Ownership.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: The ClassDojo privacy notice states that it processes personal data both as a Processor and Controller as defined in the GDPR. Where a school is entering information directly into ClassDojo the privacy notice notes that generally it will be acting as data controller. It also suggests in certain circumstances, where requested by the school, ClassDojo will be the Processor. When acting as Processor, ClassDojo will only delete records per the school's specific instructions. Any requests for access, correction or deletion of personal information can only be made through the school. ClassDojo will respond to such requests when received from the school. The school must maintain ownership of the data and this should be included in the contract.

- **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: This should be monitored to address any changes in technology and its impact on data. The school should have an understanding of the Cloud technologies used ensuring the current and future technologies enable GDPR compliance.

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

- **ISSUE:** Back up of data.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: Back up of data is stored in an alternative site and is available for restore in case of failure of the primary system.

- **ISSUE:** Security of Privacy.
  RISK: GDPR non-compliance.
  MITIGATING ACTION: The school must assess what kind of security and privacy measures are in place. ClassDojo has a US standard called iKeepSafe COPPA Safe Harbor Certification which ensures that practices surrounding collection, use, maintenance and disclosure of personal information from children under the age of 13 are consistent with principles and requirements of the Children's Online Privacy Protection Act (COPPA).

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:

- Scaleability
- Reliability
- Resilience
- Delivery at a potentially lower cost
- Supports mobile access to data securely
- Update of documents in real time
- Good working practice, i.e. secure access to sensitive files

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?

The views of senior leadership team and the Board of Governors will be obtained. Once reviewed the views of stakeholders will be taken into account

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 and Workforce). The lawful basis includes the following:

- Childcare Act 2006 (Section 40 (2)(a)
- The Education Reform Act 1988
- 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
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	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
Asset protection & resilience	Data Centre in US, Certified, Penetration Testing and Audit	Reduced	Medium	Yes
Data Breaches	Meets requirements under Privacy Shield	Reduced	Low	Yes
Subject Access Request	Meets requirements under Privacy Shield. Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Meets requirements under Privacy Shield. 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:	Claire Stylianides	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Claire Stylianides	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: Do not need to obtain parental consent to be added to system as there is a legitimate interest to using ClassDojo (homework could be shared through the system).		
DPO advice accepted or overruled by:	Yes	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Clare Benson	The DPO should also review ongoing compliance with DPIA