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. Schools may choose to operate a cloud based system or hosted solution called ClassDojo. Access to Class Dojo is through a web browser. As such each 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. Moving to a cloud service provider has a number of implications. It is essential that the school has a good overview of data privacy and information sharing potential risks.

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.

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. Every parent has the choice of whether to connect with Class Dojo or not and to create an account. No-one is forced to do so.

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 school is the data controller and ClassDojo is the data processor.

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?

Schools have an obligation to provide suitable tools to support teaching and learning, many products offer solutions. Promoting good teaching and learning is a legal duty. Achieving this aim and complying with GDPR it is possible to rely upon one or a combination of the processing principles.

1. Consent
2. Contract
3. Legal Duty
4. Vital Interests
5. Public Task
6. Legitimate Interests.

How will you collect, use, store and delete data? – The information is shared with Class Dojo when setting up an account. when setting up an account. Class Dojo lists the information that is used to set up the account and to use the service as:

- First and Last Name
- Email address
- Password
- Mobile device ID
- Gender
- Language information (native/preferred/primary language spoken by a student)
- School name
- SchoolAddress
- Local (school district) ID number
- Geolocation data (Precise)
- Photographs, videos, documents, drawings, or audio files
- IP Address (from which we can estimate a coarse geolocation)
- Browser details
- AccessTime
- Time spent on site
- Page Views
- Referring URLs
- Clicks
- Click paths
- Active/engagement time

None of these data types fall within the Section 9 'sensitive' data sets. Though they are clearly personal data.

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.

Parents and staff must be aware that this data is being used and analysed by Class Dojo. This is required as part of the contract. Which is one of the criteria for Data Processing.

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.

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

Will you be sharing data with anyone? This is a private site, that is restricted to a 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 within the same school.

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.

FROM CLASS DOJO

What Student Information is Shown Publicly?

No student's account, or Outside School Child User's account ("Outside School Child Account"), profile, or **portfolio** is made available or visible to the public through ClassDojo. Only the

student, the student's parents, and the student's teachers or school leaders can see the student's (or Outside School Child User's) profile and portfolio.

No child can upload content (such as a response to an activity, photo, video, drawing, journal entry, or document) to the Service on Portfolios except through their account. This can't happen for children without either (1) the parent providing **parental consent** directly to ClassDojo or (2) the child's teacher representing to ClassDojo that they have obtained any necessary **parental consent**, including acting as the agent of the parent if their school policy allows.

Additionally, the student's teacher **must approve** any post made by students in their Student Account (as defined below), before it is shared with parents on the student's portfolio. Parents are able to view their own child's portfolio, including any Portfolio Comments (as defined below), on their own parent account after the teacher has approved the student-submitted content.

Parents may see feedback points awarded in school if the teacher has elected to let parents see these. Parents may also award points, **goals** and **rewards** for educational and other learning activities at home through certain premium features, such as ClassDojo Beyond School **"Premium Features"** that are only viewable by the child and the child's parent(s), or those that the parent allows access to.

Class Story and **School Story** are visible by students, teachers, parents, and school leaders who have logged into their accounts and are associated with that particular class or school. They are not viewable by the general public. Parents, teachers and school leaders can add content or comments to these stories, but students can only view or like content on these stories and are only able to do this once either the school or ClassDojo has obtained parental consent, if under 13

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. Use of Class Dojo should not use special category data.

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 an optional 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 used in Class Dojo for all pupils, parents and school staff who use the system. However, this is very limited data.

How long will you keep the data for? – For the duration of their time at the school. It will then be deleted from the system, with parents and carers given notice that this will occur.

Scope of data obtained? –

All pupils
All staff who work with pupils
All parents and carers who chose to use the account

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 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) 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 processed for all children within the school setting. 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. **Encryption** Class Dojo used a sophisticated encryption system that they describe here:- ## Encryption at Rest and In Transit Access to the ClassDojo Service occurs via encrypted connections (HTTP over TLS, also known as HTTPS) which encrypt all data before it leaves the ClassDojo Service's servers and protects that data as it transits over the internet.All of our Services are in Amazon Web Services (AWS) and served from either Cloudfront or Elastic Load Balancer

(ELB). We use HTTP Strict Transport Security to ensure that pages are loaded over HTTPS connections and our TLS configuration receives an A+ from **Qualys SSL Labs**.

Student Data is stored at our Service Provider, AWS, and the following applies to their technical and organizational measures. In addition, we secure decentralized data processing equipment and personal computers. All personally identifiable information is encrypted at rest using modern encryption algorithms. In AWS S3, we use AES256 with AWS managed keys, in Aurora (MySql) we use AES-256 with customer managed keys and in Redshift we use AES-256 with AWS managed keys.

Data Controls

You own your data: We don't own any content or information you provide or we receive - you (students, parents and/or schools) will own your content and information.

Security and Privacy by Design and Default: We use security industry best practices to protect personal information, including using encryption and other security safeguards to protect personal information. We design products with security and privacy in mind from day one. See **here** for more information as well as our **Security Whitepaper** and **Privacy Center**.

Transparency and Choice: We will be transparent about our practices, so that you can make meaningful choices about how your **personal information** is used. If we make a material change, we will provide prominent notice by posting a notice on our service or this website page and/or we will notify you by email (if you have provided an email address to us). See **here** for more information.

Right to Access, Correction, and Deletion of Data: We support access to, correction, and deletion of student personal information by the student or their parent or legal guardian, either by 1) assisting the school in meeting its requirements for access, correction and deletion or by responding to requests we receive from schools, or 2) directly responding to requests from parents when the information is collected directly from a child and ClassDojo obtains the parent consent (not the school) - such as when they are using our Premium Features or Outside School Child Account. Teachers, parents, school leaders and other users can contact us at **privacy@classdojo.com** from the email used to create your account or **here** once you are signed into your account to access, correct or update their personal information, or they can use the features in their account settings to do so. See **here** for more information on all user's rights, including about your additional rights of data portability and right to object or withdrawal consent.

Data Access Control

Access to the ClassDojo Services infrastructure is highly restricted. We limit access to individuals who need access to do their jobs such as engineers, data scientists, product managers, and support personnel. All access to our infrastructure is logged. All access to our infrastructure requires the use of strong passwords and multifactor authentication.

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Student Data in accordance with their access rights, and that Student Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access personally identifiable information without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;

Using this cloud based solution raises a number of General Data Protection Regulations issues as follows:

- **ISSUE:** The cloud based solution will be storing personal data.
  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.

Whilst it is acknwoedged that the US Privacy Shield has been shot down by the EU Court, nonetheless the principles are being applied to give the greatest level of confidence that can be offered.

The nature of the data must also be a factor and in this case the material does not contain sensitive data and risk of a breach would be upsetting, but the likelihood of harm would be minimal. Considered use of the system is integral to ensuring the risk remains low.

- **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:** 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.

International Transfers

The GDPR does not forbid use of data transfers out side of the EU, it requires that suitable safeguards to deal with the level of risk and data sharing are implemented.

In this circumstance the sharing will involve US servers and be subject to US government potential review, if the conditions are met. These are considered to be National Security, terror Threat, Criminal Activity.

In this context the risk of unauthorised sharing of data held on Class Dojo is very low.

Of course, these relationships require trust. That's why every ClassDojo product is designed to protect your privacy and security, and give you control over your information. This is fundamental to our mission, and our business. Here are our promises to you:

- We don't share any of your information or students' information with advertisers or marketers.
- We don't own anything you add to ClassDojo: you do.
- Students' portfolios are private to the classroom.
- We use the latest security best practices to protect you at all times.
- We are compliant with COPPA, FERPA, and GDPR in Europe.
- We will notify you if we make any changes to our practices.

We're honored that tens of millions of you trust ClassDojo to be a part of your lives every day. Your trust means everything to us. We promise we'll always work as hard as we can to earn and keep it.

- Sam and Liam

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?

- Provision of easily accessible online learning environment
- Promote good communication between school, pupils, parents and carers
- Enable sharing that is tailored to individual children, their class and their whole school.
- Support online learning

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?

This is an offering that can be reviewed. As it is an effective and well established platform we are not proposing to consult.

Parents choose to sign up. If they choose not to do so information will eb provided in an alternative format.

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 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.

Our basis for processing and choosing to use this method is also linked to the legal Direction issued by the Secretary of State for Education in October 2020 that requires schools to offer a suitable online learning environment.

Also parents and carers must consent to use the system, and have he opportunity to refuse to sign up.

We also have a legal duty to facilitate teaching and learning.

There is a contractual element, although the basic system is free.

As a school there is also the broader legitimate interest point that we are expected to use available tools to support our pupils and school communities.

Step 5 & 6: Identify assess and reduce risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.
Data transfer; data could be compromised Use of encryption limits this risk. Every data transfer contains an element of risk. The use of robust encryption methods is an acknowledged method too limit risk. It is important that Class Dojo continue to take the necessary steps to monitor and develop their protection and security matches to reduce this risk Usage It is necessary that staff training is undertaken, with an emphasis on GDPR compliance and awareness of using the data minimization principle to reduce the amount of information that is shared on class Dojo, without reducing its effectiveness. Misunderstanding of the product, over sharing information errors are an inevitable risk for any user. Data Breaches I tell you to breach my account if information is posted about the child on the wrong account. Every school user must be aware of the potential implications of doing this . As this is a learning tool, consideration should be given to the type of information that is shared across the system. Subject Access Request All school staff should be aware that Information they place onto the system may be subject to a subject access request. staff should be aware of the subject access request protocol and process that can be deployed to support a data subject making a request. Data Retention It is important that the retention scheme is applied to this material.

Step 5 & 6: Identify assess and reduce risks

Application of good GDPR principles, that include internal and external security measures, data minimisation and improved staff awareness and training will all assist to reduce risks.

the fact that the programme shares data with a US faced server is an increased risk factor, but this must be balanced against the effectiveness of the product and the type of data that is being shared.

Data shared using class Dojo relate largely to pupil, parent, carer and staff names and addresses.

Material that is uploaded will include teaching and learning materials, class work , pictures and photos. Of course, use of class Dojo must be monitored by school staff. This is the greatest way of reducing risk as any inappropriate or unsuitable information material will be removed.

Whilst pupils behaviour camera be reported using this system it is likely that any significant concerns would be dealt with separately .

Start awareness will be the key.

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Headteacher
Residual risks approved by:		Head and SLT/IT support if concerns about particular elements of the product
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: When reviewing and assisting to prepare this DPIA, I have taken into account the fact that this is a US based programme. I have also considered the information that needs to be shared , and I am satisfied that the only information that classdojo requires is personal data that does not fit within the sensitive /special category classification's . All schools are now under a duty to provide a remote learning platform. Class Dojo is a tried and tested service come up with a comprehensive privacy and security policy Parents and carers are given the option to sign in and access information contained in class Dojo. My recommendation is that if any parent or carers chooses not to do this, alternative methods of providing similar information must be available. However, this does not mean that they will be as fulsome or detailed as material provided on Class Dojo. It is essential that staff understand they have a personal responsibility when considering what information should or should not be shared on this platform. Whilst there are risks with this platform, that are risks with any online learning platform. Another advantage of class Dojo is that it is intuitive to use, which will be likely to reduce risk of user error that may lead to unauthorised sharing all personal data .		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons

Step 7: Sign off and record outcomes

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:		The DPO should also review ongoing compliance with DPIA