



DPIA – Class Dojo

Version 6.0

Name of School	Chinley Primary School
Document Prepared by	Claire Archibald, DPO, Education Data Hub
Reviewed by DPO	Yes- Claire Archibald
Date of DPO review (see DPO Cover note below)	11/1/24
Governor minute number/reviewed by SLT	Reviewed by SLT
Governor/SLT Review Date	11.01.2024

DPO Cover note:

Based on the information available at the time of writing and the checks made on the provider's documentation the DPO is satisfied that this DPIA addresses the main data protection risks of using this provider. The school should ensure that the mitigation actions set out in the risk table below are carried out by the appropriate member of staff. The DPO can support the school staff with the actions upon request.

The DPO draws attention to these key areas:

- 1) Setting up parent accounts, messaging parents and the automatic sharing of contact information with other users and Class Dojo brings up a number of privacy issues. The DPO notes that the school does not use this functionality and therefore this reduces risk considerably;
- 2) In relation to the storage of data in the USA- ensure that the Student and International Data Processing Addendums are signed and that governors/leaders read and understand the advice of the DPO in relation to the reliance on the DIST analysis in place of a full Transfer Risk Assessment; and
- 3) carefully consider exactly which data sets should be shared with Dojo and ensure that only those necessary are shared.

There are more detailed DPO Advice Notes in relation to these points at the appropriate place in this document (see orange boxed text).

Version History			
Version	Date	Detail	Author
1.0	January 2024	First DPIA for this processing by this school	Claire Archibald, DPO and Peter Lambert, HT

Introduction

Class Dojo is a popular and well-used web-based application used in schools to process the progress of pupils and share information directly with parents/carers (referred to as 'parents' throughout this document). The application is used for all school pupils and connects with parents via a log in or app. Particularly since the pandemic, Class Dojo has been used as the communication tool of choice for a very large number of UK primary schools and nurseries.

Class Dojo are a data processor for data that is input by the school and parents for use of the platform in a school context (they may act as data controller for data that is input by parents where they purchase additional Outside School Account features of the platform- this is outside of the scope of this DPIA).

Class Dojo provides the following through its platform:

- A way for teachers to give feedback and assignments to students, and other classroom management tools
- Communication tools to help teachers and parents connect with each other
- A way for teachers to share photos, videos, files, and more from the classroom for parents and students to see
- Student portfolios, where students can share their work with teachers and parents
- Activities and other content that teachers or parents can share with students
- A way for school leaders to see how connected their school community is, and also to communicate with parents.

Primarily, Class Dojo is a school communication platform that helps teachers encourage students in class and engage parents. Initially, the system is often first procured for teachers to use Class Dojo to give students encouragement (or "feedback points/Dojo points") for showing critical skills or strengths. This is often the beginning of a gradual further adoption of further functionality- the software is enticing and attractive, and without controls, it is quite likely that there will be 'scope creep' for schools that use Class Dojo once embedded in a school's culture.

This is the first time that the school have considered the use of Dojo in a DPIA but the system has been in place for some time.

At Chinley School, although we acknowledge the various range of applications available through Class Dojo we ONLY use the system as a record of rewards in a points gaining system towards individual and group rewards. At Chinley School NO parents have access to the system and staff are aware that if they are contacted through the site by parents asking to be accepted for access they MUST refuse.

This Data Protection Impact Assessment will consider the suitability of the software for the intended purpose, how the school will use Dojo to ensure adherence to Data Protection Laws and the steps the school will take, what data will be shared, and evidence the due diligence process undertaken.

Creating accounts and using Class Dojo

There are several implications to setting up and using accounts. Each of these has a privacy 'pinch point' (**indicated in bold**). The only implications for Chinley School are recorded below:

1. A teacher, school leader, admin staff member or parent sets up a new school account, or links to an existing school account. **Dojo automatically collects the precise geolocation of users at that point (there is no option to decline this)** which they state helps "*us to identify*

schools located nearby for you, including to help connect your parent account to your child's school (e.g. our "find a teacher" feature). This location data is only temporarily captured"

2. a. On the platform, a teacher, school leader or admin staff member enters the class and first and last names of students in their school.

b. parents **(or any person)** can download the Class Dojo from their app store, create an account and then search for their local school and choose their child's teacher from within the list shown within Class Dojo App or Class Dojo Website (the request to join the class must still be approved by the teacher). **It is therefore possible for anyone to search for schools, and easily find information about which teachers work at the school (and view their profile picture).** We do not accept any requests to join the group.

Class Dojo can be accessed via web browser or via mobile phone app. **Schools should consider whether teachers are permitted to use their own mobile phones for work purposes and the school IT Acceptable Use Policy should be amended accordingly.**

DPO Advice Note

Setting up Dojo and inviting parents to link with the school brings up a number of privacy issues, the DPO has drawn these to the Headteacher's attention. These are important issues to consider- particularly whether parents would expect their personal data to be used and shared in this way. Data processing must be fair- would parents expect their personal data to be shared with others for the purpose of the school communicating with parents?

If the school decides to enable parents to access Dojo, then the risks should be fully explored and mitigated by revisiting this DPIA. The school would also need to ensure at that point that they:

1. Are clear with parents about how their data is shared, and ensuring that they have a genuine choice whether or not to use Dojo (and ensuring they can still receive messages if they choose not to create a parents account)
2. Carefully train staff and explain to them how the features work (such as the potential for anyone to find their name and profile picture and the ability for parents to obtain read receipts) and by carefully considering whether additional features such as the Dojo island should be permitted.

Why do we choose to use Dojo?

Class Dojo provides a visual and fun method of rewarding pupils for their hard work, kindness, efforts, etc. in the classroom and around school.

The system motivates pupils to make good choices and provides the class teacher with opportunities to publicly reward pupils for what they do.

The system of rewards provides in-class rewards which motivates the pupils. They like the cartoon avatars and the watching their Dojo points grow towards rewards.

We do not accept requests from parents to access the Dojo records and staff are aware of this; there is no use of the messaging facility.

Describe the nature, scope and context of the data processing

Whose data will be collected?

Pupil and staff personal data will be collected as set out in the table below:

Types of data	Yes	No	Types of data	Yes	No
Name	x		Sex life or sexual orientation		x
Date of Birth		x	Looked after status/ previously in care		x
Email Address/ IP address		x	Health Data (Education and Health Care Plan)		x
School attended/ class		x	Race		x
Contact telephone number		x	Ethnic origin		x
Gender		x	Political opinions		x
Profiling/analytical/insights information/cookies		x	Religious or philosophical beliefs		x
Photograph/film footage		x	Trade Union membership		x
Banking details		x	Genetic data		x
Card payment information		x	Biometric data (where this is used for identification purposes)		x
Salary/employment benefit details		x	Criminal Offence data		x
Vulnerable adult data		x	Free School Meals status (including FSM6)		x
Children's data		x	SEN status/support		x
Pupil UPN		x	Other – children's attainment Messages between parents and school (which may contain any personal data- school cannot stop parents from including confidential information in a message) See https://www.classdojo.com/en-gb/transparency/?redirect=true for details of IP address/Browser Type/Access and Active Time/Clicks/Page views		x

Will the project involve the collection of new information about individuals? If yes, please detail the information to be collected.

There will be no collection of new information, the information is already collected and maintained in the school using different methods. The change is who this information is shared with, namely a new Data Processor.

What is the lawful basis of the processing of this data?

The lawful basis for processing data to reward pupils for their work, kindness efforts etc is a public task duty for the education of pupils as a necessary part of that provision of education is providing pupils with clear feedback about expected behaviours.

DPO Advice Note

Schools should always be cautious when sharing personal data with external providers. In order to be compliant with Data Protection laws, schools should ensure that only the minimum amount of personal data is shared. It is particularly important to note that the Dojo Data Processing Agreement states that the school “shall not provide any special categories of Personal Data... which is for the sake of clarity Personal data with information revealing racial or ethnic origin...data concerning health or data concerning a natural person’s sex life or sexual orientation”

No special category data is intended to be processed in the limited use of this platform.

Will the project compel individuals to provide information about themselves? If yes, please detail the information to be provided.

No

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? If yes, please detail which organisations will be provided with access.

Yes, information is held by Class Dojo, a new provider, and their service partners (who may be acting as sub-processors), as described in their privacy notice.

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? If yes, please describe the new purpose below.

No.

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. If yes, please detail the new technology, below.

No.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? If yes, please describe the impact, below.

No.

Will the project require you to contact individuals in ways that they may find intrusive? If yes, please describe how the individuals will be contacted, below.

No

How and where will the data be stored?

According to the Dojo Terms, the data will be stored in servers in the USA. This means the use of Dojo involves “International Data Transfers” to a country without an “Adequacy Decision”.

DPO Advice Note

Class Dojo is a US Based company and personal data will be stored in the USA. Data Protection Laws state that appropriate safeguards must be in place for international transfers to countries outside the EEA.

Whilst the ‘safest’/most risk averse option regarding data protection would be to not use Dojo (replacing it with a provider where data is stored in the UK or EEA), the [DfE](#) has made it clear that schools should use digital tools as part of their teaching and learning strategy. Setting up new platforms requires financial and time investment which is not currently possible in most schools. Dojo can be set up relatively easily by schools without financial expenditure.

There are strict legal requirements for transfers to US companies. In October 2023, the UK introduced a mechanism for UK controllers to rely on an EU-US “data bridge” in the form of the “UK Extension to the EU-US data privacy framework”. This allows the free flow of personal information to US recipients that are appropriately certified under the scheme. ClassDojo complies with the EU-U.S. Data Privacy Framework and the UK Extension and is certified accordingly.

Transfer Risk Assessment (TRA)

Additionally, the ICO state that a “Transfer Risk Assessment” must be carried out. The aim of this exercise is for organisations to consider the risks relating to the international data transfer; whether the legal document used (in this case the “International Data Processing Addendum”) would actually be enforceable in the destination country and to consider the destination country’s regime and whether it is sufficiently similar in its objectives to the principles which underpin UK laws. The ICO has produced [guidance](#) on this. Dojo has also provided their own Transfer Risk Assessment which provides useful information:



ClassDojo Transfer
Impact Assessment (T

Dojo has also provided a Security Whitepaper (see Appendix A below) and a Security Risk Assessment (see Appendix B below).

Completing a TRA is a specialist task, usually undertaken by specialist lawyers. The DPO notes that even the ICO recently appointed lawyers to carry out a TRA for them. The DPO Service provided by the Education Data Hub excludes the preparation of TRAs, as these are large items of work, requiring expert knowledge of another country’s laws and would take many hours to complete. If the school requires a TRA to be carried out, then the DPO can support the school to procure this advice, at the school’s expense.

However, the work undertaken to establish the UK extension to the EU-US data bridge included a detailed analysis by the UK Department of Science, Industry and Trade (DSIT) of the level of protection that the US gives people in the UK. DSIT’s review took into account:

- the rule of law;
- respect for fundamental rights and freedoms;
- the existence of an effective and independent supervisory authority; and
- relevant international commitments.

DSIT concluded that the US data bridge and other relevant US laws and practices provide an adequate level of protection for UK personal information. They do not undermine the level of protection that people in the UK enjoy under the UK GDPR, when that personal information is transferred to certified US organisations.

In considering the required Transfer Risk Assessment, the DPO advises that the ICO states that it is [acceptable for data controllers to rely](#) on the DSIT’s [Analysis of the UK Extension to the EU-US data privacy framework](#) published in September 2023 (the DSIT analysis).

The school may be satisfied that the DSIT analysis concludes that US laws and practices provide adequate protections for people whose personal information is transferred to the US for risks to people’s rights:

- arising in the US from third parties that are not bound by the Dojo SCC's with UK Addendum accessing the transferred personal information in particular, government and public bodies; and
- arising from difficulties enforcing the SCCs with UK Addendum,

and that therefore a full TRA is not required. The DPO advises that it is reasonable and proportionate for schools to rely on the DSIT analysis, given the scope of this assessment is as required under Article 45 UK GDPR, and the enactment of adequacy regulations under Section 17A DPA 2018 by the Secretary of State and Parliament, on the basis of that assessment. Other aspects of the TRA are considered throughout this DPIA and a separate full TRA would be a duplication of the DPIA work.

The DPO will advise a review of this if a new or amended version of the DSIT analysis is published, or the DSIT analysis is withdrawn.

The Dojo Transfer Risk Assessment, the DSIT analysis and this DPO Advice Note may be accepted by School Governors/Leadership as a proportionate investigation into the risks relating to the international transfer, instead of carrying out a separate TRA.

How many individuals are likely to be affected?

Staff and pupils.

How long is the data kept for?

The school will retain data in line with their normal data retention policy. Dojo should return or delete any data at the end of the service contract. It is important for schools to ensure that Dojo does not retain any data for longer than the school's own retention period.

Will training and instructions be given to appropriate staff to ensure compliance with policy and procedure?

Yes. Staff have access to help articles and can email Class Dojo for support.

Note regarding Consultation

The school will consult with the Data Protection Officer and Governors regarding the use of this provider.

Conclusion regarding need for a DPIA

The use of the platform is not considered to be a novel or risky new use of data in itself.

Describe the information flows

Individual teachers who choose to use the Class Dojo as a reward system register their class and upload the names of the children in their class. No access is allowed for parents.

Account Level	School Leader/Class Dojo Mentor	Teacher	Student	Parent Account
Personal Data on Platform to set up account	None	First name, surname, email address	First name, last name (or surname initial)	None
Personal Data created on Platform	None	None	None	None
View level of access	None	Can view all content for their class	View the number of points they have earned.	None

Ability to amend/delete data	None	Teachers can delete their own account and content.	None	None
-------------------------------------	------	--	------	------

Identify the privacy and related risks and mitigations

Data Protection Principle	Description and mitigation in place	Further mitigation actions that must be carried out by the school	Person responsible and if applicable, date of completion
Lawfulness, fairness and transparency.	The lawful basis for the sharing of data is Public Interest.	None	n/a
	The processing should be fair-sharing personal data in this way should be fair (and expected). Parents and pupils expect their personal data to be shared with some external companies in order for learning to take place.	Carefully consider the DPO advice in relation to not allowing parents access to this platform- if this is decided to be done then the DPIA will need to be revisited. Add the processor or the type of processor to the privacy notices, if not already included. Ensure privacy notices are accessible to data subjects.	Peter Lambert
	Data subjects have a right to be informed- the processing will be transparent if the school ensures that the relevant Privacy Notices are updated to include information relating to this processing activity. Data Subjects must be informed that there is an International Data Transfer taking place.	Ensure relevant Privacy Notice(s) are updated with details of who the data is shared with and that there is an international data transfer. There is also a privacy video for children which is a useful tool to discuss Dojo and privacy with pupils- https://vid.ly/6l7i1p	Peter Lambert
	Data Subjects must be able to exercise their rights under data protection laws. The rights are already available to data subjects and are explained in the privacy notices-	Ensure that the privacy notices are up-to-date and easily available for data subjects (e.g. on school website)	Peter Lambert

Data Protection Principle	Description and mitigation in place	Further mitigation actions that must be carried out by the school	Person responsible and if applicable, date of completion
	these rights are extended to the data shared/processed for this project (and documented in the contract).		
Purpose limitation.	Personal data will be shared for the purpose of this processing activity- the school will not use the personal data for any other purpose beyond what it already does or reasonably needs to in pursuance of ensuring pupil attendance and safeguarding. Dojo has confirmed that personal data will only be used for the purposes set out in the Data Processing Addendum and their Privacy Notice.	School relies on external providers documentation giving assurances regarding the processing of personal data for this purpose only. Dojo state that they will enter into Student and International Data Processing Addendums- see the due diligence section below for the links to these and a link to complete and sign these documents electronically- ensure this is done by an appropriate member of school staff and a record is kept of the signed document.	Peter Lambert
Data minimisation.	The data of children should be kept to the minimum possible in order to use the product.	Ensure that only data sets that are strictly needed are shared with Dojo. Review data sets collected and check regularly. Keep this under review to ensure only minimal data is being collected and processed. Ensure that no special category data is shared in order to minimise the risk to privacy and to comply with the contract with Dojo. Staff must be told not to include any special category data on pupil comments or accounts.	Peter Lambert
Accuracy.	The school is responsible for ensuring personal	Nominate member of staff responsible for ensuring personal data is regularly checked for accuracy.	Peter Lambert

Data Protection Principle	Description and mitigation in place	Further mitigation actions that must be carried out by the school	Person responsible and if applicable, date of completion
	data is accurate and up to date. All staff have a responsibility to ensure that data is factually correct.		
Storage limitation.	Storage of this data is already addressed as part of school retention policies. Dojo state in contract documentation and in communications with the DPO that data will not be deleted unless on the instructions of the school.	Ensure staff member deletes or destroys data no longer needed- whether stored on external services or internal systems. Ensure Dojo delete or destroy all data at the end of the service contract and in line with school retention periods. This means that when a pupil leaves the school, the school will need to take active steps to remove a child's/parents data from the platform. Deletion requests must be sent to privacy@classdojo.com (or sent via dedicated URL https://www.classdojo.com/en-gb/datasubjectrightsrequest/?redirect=true)	Peter Lambert
Integrity and confidentiality (security)	There is a medium risk that this processing could result in a data breach that users of the platform, school staff, the external providers or unknown external actors could be responsible for. A Data Processing Agreement (DPA) is necessary for this project. The law states that this document should contain key terms. The checklist in the DPA Appendix set out which terms are required and where they are in the documentation.	Ensure all school staff comply with instructions and guidance regarding data protection and IT usage. The school has limited risk by instructing staff not to use Dojo to communicate with families. Ask your IT manager/specialist to set out what technical safeguards can be put in place to ensure that cyber risk of using this product is mitigated. If Google Login is used, then Dojo states this is the responsibility of the school. Enter into Data Processing Addendum agreements with Dojo and retain a copy of all documentation.	Peter Lambert

Data Protection Principle	Description and mitigation in place	Further mitigation actions that must be carried out by the school	Person responsible and if applicable, date of completion
	The school is responsible for ensuring their staff comply with Data Protection requirements. Dojo is also responsible to the school under the terms of the Data Processing Addendums.		
Accountability.	All parties have responsibilities to account for their data protection practices. This DPIA and the documents referred to in this document form part of the accountability practices of the school. Dojo have committed to accountability/ liability for the acts of their sub-processors in contract documentation.	Retain evidence of work done to comply with Data Protection laws. Keep this DPIA under review over time as use of the platform may change in the future. Ensure description of this processing is included in the school data map/RoPA (use GDPRiS for this).	Peter Lambert

Risk Rating Decision

Once all the privacy risks and mitigations have been addressed as above, the overall level of residual data-related risk is low **after the mitigation actions have been carried out, and the recommendations followed**. The school leadership and governance should note this risk and if appropriate, include it in the Information Risks section of the School/Trust Risk Register. Keep this document under review and check use of Dojo products is in accordance with the intentions set out in this document.

Risk Register Advice Note

It is good practice for schools to have risk registers. Risk is an inherent part of school practices and it is important that risk management is part of governance and leadership. Academy trusts in particular **must** maintain a risk register, see

<https://www.gov.uk/government/publications/academy-trust-financial-management-good-practice-guides/academy-trust-risk-management> for more information.

In addition, the Information Commissioner's Office (ICO) recommends that information (data protection and IT security) risks are managed using a risk register. The ICO provides guidance in the form of a good practice study as part of their investigation into data protection compliance in Multi Academy Trusts https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618610/mats-outcome-report-v1_1.pdf (page 6)

Appendix A: Evidence of due diligence

As the Data Controller, the school may only rely on an external data processor if it provides sufficient guarantees in relation to appropriate controls and GDPR compliance. The statements at the weblinks below have been checked by the School and the Data Protection Officer:

External Provider Name and Address	Class Dojo Inc 735 Tehama Street San Francisco, California, 94103 United States of America
External Provider ICO Number	Not applicable
External Provider DP Contact Details	privacy@classdojo.com
Privacy Notice	https://www.classdojo.com/en-gb/privacy/?redirect=true (version dated 05/10/23 checked by DPO on 20/12/23) Privacy video for children (you may wish to share this with your pupils) https://vid.ly/6l7i1p
Contract/Data Sharing Agreement	DPO Advice Note: Existing Contracts: If you entered into Dojo UK International Student Data Processing Addendum prior to September 21, 2022, you will have entered into SCCs with ClassDojo ("Prior UK DPA"). For any UK school that previously contracted with ClassDojo with the Prior UK DPAs, these contracts are still valid until March 21, 2024. New Contracts: ClassDojo currently offers an International DPA and relies on the UK Extension and will no longer rely on the UK Addendum as the transfer mechanism. For any new contracts, there are two documents that should be signed- • ClassDojo's Student Data DPA can be viewed at the link and signed digitally here. • ClassDojo's International DPA can be viewed at the link and signed digitally here.
Terms of Use	https://www.classdojo.com/en-gb/terms/?redirect=true (version dated 16/10/2023 checked by DPO on 04/01/2024)
Any additional information	DPO and Dojo have been in long term communication regarding compliance with UK Data Protection laws. Copies of these communications are available upon request. https://classdojo.zendesk.com/hc/en-us/articles/360053338371-Transfer-of-Personal-Data-to-the-U-S- https://www.classdojo.com/en-gb/privacycenter/?redirect=true https://www.classdojo.com/en-gb/security/?redirect=true

Checklist for Data Processing Agreement with Dojo

(checked by DPO 04/01/2024)

A Data Processing Agreement must set out:	Included in Student Data Processing Addendum	Included in International Data Processing Addendum
The subject-matter of the processing	Exhibit A- clause 2	Schedule 2 B.6
How long the processing will continue for	Recitals- 3 years	Schedule 2 B.7
The nature and purpose of the processing	Recitals- refers to Service Agreement and Exhibit A clause 2	Schedule 2 B.5
The type of personal data	Schedule of Student Data	Schedule 2 B.2
The categories of data subject	Schedule of Student Data	Schedule 2 B.1
The controller's obligations and rights	Exhibit B- Clause 3 "Duties of LEA"	Clause 2.2
The processor will only process the personal data in accordance with our written instructions, unless required to do so by law	Exhibit B- Clause 4.2	Clause 2.3
The processor must obtain a commitment of confidentiality from anyone it allows to process the personal data, including staff, agency workers and volunteers.	Exhibit B- Clause 4.3	Clause 6.1
The processor must put in place appropriate technical and organisational measures to ensure the security of any data they process	Exhibit B- 5.3	Clause 8
The processor must assist the controller and also to take "appropriate technical and organisational measures" to help the controller respond to requests from individuals to exercise their rights.		Clause 3
The processor will notify the controller of any personal data breach without undue delay	Exhibit B- Clause 5.4	Clause 9
To assist with any Data Protection Impact Assessment		Clause 4.1
The processor to provide the controller with all the information that is needed to show		

A Data Processing Agreement must set out:	Included in Student Data Processing Addendum	Included in International Data Processing Addendum
that the obligations of Article 28 have been met; and		
The processor to allow for, and contribute to, audits and inspections carried out by the controller, or by an auditor appointed by the controller.	Exhibit B- Clause 5.2	Clause 8
at the controller's choice, delete or return to the controller all the personal data it has been processing for it; and	Exhibit B- Clause 4.6	Clause 11
delete existing copies of the personal data unless EU or Member State law requires it to be stored.	Exhibit B- Clause 4.6	Clause 11
The Processor must not use another processor (a sub-processor) without the controller's specific or general written authorisation		Clause 7.3 and 7.4
If a sub-processor is engaged, there must be a contract in place which gives effect to terms substantially similar to the one between the controller and processor	Exhibit B- 2.5	Clause 7.2
if a sub-processor is employed under the controller's general written authorisation, the processor should let the controller know of any intended changes and give the controller a chance to object to them		Clause 7.4
The processor is liable to the controller for the sub-processor's compliance with its data protection obligations		Clause 7.5

Appendix B: Security Risk Assessment Response from Dojo

Is ClassDojo subject to FISA Section 702?

ClassDojo is subject to the Electronic Communications Privacy Act ("ECPA") which affords privacy protections to individuals, including requiring the U.S. government to seek heightened legal process in order to access the data of our users'. Because ClassDojo is subject to ECPA, we are potentially subject to Section 702 of FISA.

What is the risk for ClassDojo to receive Section 702 FISA Requests?

ClassDojo is extremely low risk for receiving any Section 702 FISA request given the type of platform and communities it connects (teachers, students and families), as well as the type of data that it processes. For full background, ClassDojo has never received a Section 702 FISA request to date. Of note, since we founded ClassDojo, we have received fewer than 10 U.S. governmental requests for any type of legal process (outside of Section 702) to obtain user data from the ClassDojo services.

What measures will ClassDojo take if it were to be served with a FISA 702 request?

If ClassDojo were to receive a Section 702 FISA request and was also unable to demonstrate full compliance with the European Commission's Standard Contractual Clauses ("SCCs), ClassDojo would inform the relevant data exporter.

In addition, ClassDojo has implemented the technical and organization measures set forth in our Security Whitepaper (see below). These measures include encryption of personal data in transit and at rest.

ClassDojo does not voluntarily cooperate with any U.S. government agency—and has not been compelled by any U.S. government agency—to provide data pursuant to Executive Order (EO) 12.333 and has encrypted data at rest and in transit in order to prevent any attempts to obtain its data through other surveillance activities.

ClassDojo Security Whitepaper

ClassDojo, operates the services offered on classdojo.com (the "ClassDojo Website"), including the ClassDojo platform (the "ClassDojo Platform"), and any associated mobile applications (the "ClassDojo Apps") or products and services that Company may provide now or in the future (collectively, the "Service").

Protecting data privacy and security is a top priority for ClassDojo. Our [Privacy Policy](#) and [Student Data Privacy Addendum](#) solidify the commitments that ClassDojo and schools make to each other, including our security and privacy commitments. Capitalized terms not defined in this document, such as "Student Data", are defined in our Student Data Privacy Addendum. We regularly evaluate our policies and practices to improve security and to keep up with the latest practices of the security industry.

This document is designed to provide technical readers, such as Chief Information Officers or Chief Technology Officers at school districts, additional clarity and specifics about our security commitments. While this document is written for technology experts who often play a key role in assessing our policies, we recognize that data security is just as important to families, teachers, and students as it is to school officials. If you would like to find out more and access materials that are written to help you digest the more technical information here, please visit our [Privacy Center](#). Additionally, should you have security or privacy questions, please reach out to our team at privacy@classdojo.com

Infrastructure Security

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. Additionally, we use MongoDB with AES-256 with keys managed by AWS. For more information on these vendors please see our [Third Party Service Providers chart](#).

Network Security

The ClassDojo Services use AWS, to host the infrastructure. AWS undergoes strict ongoing security assessments from external audit firms to ensure compliance with security standards including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. See <https://aws.amazon.com/compliance/programs/> for more details.

Network access to the ClassDojo Services infrastructure is highly restricted. AWS hosted infrastructure resides in a dedicated Virtual Private Cloud (VPC) which is designed to ensure that only authorized traffic over approved ports is allowed. We use ThreatStack to monitor for suspicious activity.

Patching

We use automated processes to regularly install security updates on the infrastructure that powers the ClassDojo Services, these processes include:

- AWS Managed Services (e.g., Relational Database Service):** AWS proactively notifies our engineering team when updates are available and we apply them in a timely fashion.
- AWS EC2:** All EC2 instances are monitored by ThreatStack and AWS inspector and updates are applied in a timely fashion
- Classdojo Application:** Monitored by Snyk.io and Github for vulnerabilities and they are updated in a timely fashion

Backups and Availability Control

We have a data backup and recovery capability that is designed to provide a timely restoration of the ClassDojo Services, with minimal data loss, in the case of catastrophic failure. These backups are encrypted and stored in multiple availability zones. Additional technical and organizational measures to ensure that Student Data are protected against accidental destruction or loss (physical/logical) include:

- Uninterruptible power supply (UPS);
- Remote storage; and
- Firewall systems.

Note: Student Data is stored at our Service Provider - currently AWS - and the above applies to their technical and organizational measures as well as any other relevant [Service Providers](#), such as MongoDB. In addition, we have a disaster recovery plan in place.

[Physical Security](#)

Physical Access Controls

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Student Data are Processed*, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);and
- Surveillance facilities, video/CCTV monitor, alarm system.

Note: The ClassDojo Services are currently hosted in AWS and Student Data is stored at our Service Provider - currently AWS – which employs industry- leading physical security measures to protect their data centers and the above applies to their technical and organizational measures. These security features are regularly audited by third party auditors. You can learn more about AWS' physical security [here](#). We also utilize MongoDB. You can learn more about Mongo DB's security [here](#). In addition, we secure decentralized data processing equipment and personal computers.

Virtual Access Control

Technical and organizational measures to prevent data processing systems used for Student Data from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password); and
- Encryption of archived data media.

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.

Disclosure Control

Technical and organizational measures to ensure that Student Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Student Data are disclosed, include:

- Encryption/tunneling;
- Logging; and
- Transport security.

Entry Control

Technical and organizational measures to monitor whether Student Data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems; and
- Audit trails and documentation.

The Data Protection Officer has assessed this information against the European Data Protection Board's advice at

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf and considers that the technical measures listed above give some level of assurances about the safety of data being adequately protected.

The DPO also notes that there is a great degree of concern regarding the potential for US Government Institutions to gain access to EU Citizens data (and that formed a central reason for the invalidation of the Privacy Shield). The International Data Processing Agreement and SCCs contain the following provision which contains as much assurance as possible in this situation:

*“Unless prohibited by EU or EU member state law, and subject to the procedures set forth in Section 2.5 of the Student DPA (“**Third-Party Request**”), ClassDojo must promptly inform LEA if ClassDojo receives a request to disclose Personal Data from law enforcement, courts or any government entity; is subject to a legal obligation that requires ClassDojo to Process Personal Data in contravention of LEA’s instructions; or is otherwise unable to comply with Data Protection Laws and Regulations or this Int. DPA. If ClassDojo is prevented from notifying LEA as required under this Int. DPA, ClassDojo must consult and comply with the instructions of the competent Supervisory Authority.”*

Appendix C: Data Sets that may be shared with Dojo

Category of Data	Elements	Check if used by your system
Application Technology Metadata	IP Addresses of users, Use of cookies etc.	✓
	Other metadata; see here: https://www.classdojo.com/transparency	✓
Application Use Statistics	Metadata on user interaction with application	✓
Assessment	Standardized test scores	N/A
	Observation data	✓
	Other assessment data-Please specify:	N/A
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	✓ if teachers elect to record
Communications	Online communications that are captured (emails, blog entries)	✓ Not from students, unless they message directly with their teacher in Portfolios
Biometric Data	Physical or behavioral human characteristics that can be used to identify a person (e.g. fingerprint scan, facial recognition)	N/A from students; may use to validate parents/teachers with iOS or Android technology - we are not passed the information
Conduct	Conduct or behavioral data <i>For ClassDojo: "Feedback points" are added by the student's teacher</i>	✓
Demographics	Date of Birth <i>For ClassDojo: This is collected as an age, not DOB</i>	✓
	Place of Birth	N/A
	Gender <i>For ClassDojo: We ask adults for an optional Mr./Miss/etc. salutation</i>	✓ not from students
	Ethnicity or race	N/A
	Language information (native, preferred or primary language spoken by student) <i>For ClassDojo: This is obtained via browser/device preferences</i>	✓
	Other demographic information	N/A
Enrollment	Student school enrollment	✓
	Student grade level	✓
	Homeroom	N/A
	Guidance counselor	N/A
	Specific curriculum programs	N/A
	Year of graduation	N/A
	Other enrollment information-Please specify:	N/A
Parent/Guardian Contact Information	Address	N/A
	Email	✓
	Phone	✓
Parent/Guardian ID	Parent ID number (created to link parents to students)	✓
Parent/Guardian Name	First and/or Last	✓
Transcript	Student course grades	N/A
	Student course data	N/A
	Student course grades/performance scores	N/A
	Other transcript data -Please specify:	N/A

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	N/A
	Teacher names	✓
Special Indicator	English language learner information	N/A
	Low income status	N/A
	Medical alerts	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information-Please specify:	N/A
Student Contact Information	Address	N/A
	Email	✓ only for students whose teachers elect to utilize Google Login
	Phone	N/A
Student Identifiers	Local (School district) ID number	✓
	State ID number	N/A
	Vendor/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last <i>For ClassDojo: option to only share last initial</i>	✓
Student In App Performance	Program/application performance (e.g., typing/reading program performance)	✓ We track product events and progress within a particular function for internal product usage analysis
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	N/A
Student Survey Responses	Student responses to surveys or questionnaires	N/A
Student work	Student generated content; writing, pictures etc. <i>For ClassDojo: this may also be teacher assigned projects</i>	✓
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A
	Student bus card ID number	N/A
	Other transportation data - Please specify:	N/A
Other	Please list each additional data element used, stored or collected by your application	**

** Please see the Information Transparency Chart located at:

<https://www.classdojo.com/transparency> for additional details:

- 1) Categories of Student Data
- 2) Categories of Data Subjects the Student Data is collected from and the source of the Student Data
- 3) Nature and purpose of the Processing activities of the Student Data
- 4) Country in which the Student Data is stored
- 5) List of any Special Categories of Student Data collected (currently none)

The current list of Service Providers is located at:

<https://www.classdojo.com/third-party-service-providers/>