DPIA

Introduction

This document presents a Data Protection Impact Assessment (DPIA) for ClassDojo, an educational platform widely used in the UK. The DPIA is crafted in accordance with the General Data Protection Regulation (GDPR) principles to provide a comprehensive overview of ClassDojo's data processing operations, the necessity and proportionality of such processing, the potential risks to individuals, and the mitigating measures employed. The assessment underscores ClassDojo's commitment to user privacy and its continued compliance with pertinent data protection regulations.

A description of the processing operations and the purposes

- **Collection of personal data:** ClassDojo collects data from users (both educators and students) such as names, school details, email addresses, and usage data.
- **Processing for educational purposes:** The platform processes the data to facilitate communication between teachers, students, and parents, and to support learning through gamification and interactive features.
- **Data storage:** The data collected is stored on secure servers which can be located in and outside the UK.
- **Data sharing:** Certain data may be shared with third-party service providers for the purposes of system maintenance, analysis, and improvement. All third-party service providers are contractually obliged to ensure the safety and privacy of data shared with them.

An assessment of the necessity and proportionality of the processing in relation to the purpose

- **Necessity:** Collecting basic user data is necessary for the provision of ClassDojo's services. This includes enabling account creation, personalising user experience, facilitating communication, and ensuring the functionality of the platform.
- **Proportionality:** The data processed by ClassDojo is proportionate to its educational and communication aims. Only data that is essential for providing and enhancing these services is collected and processed. No excessive data is gathered.

An outline of the risks to individuals & The measures implemented in order to address risk

Issues	Mitigating Actions
Data Breach: Risk of a data breach leading to unauthorised access to personal data.	Security measures: Implementation of strong security measures like encryption, firewalls, and SSL technology.

Misuse of Data: Potential misuse of personal data by internal staff or third-party providers.	Data Minimisation: Only necessary data is collected, processed, and stored.
Non-Compliance: Risk of non-compliance with data protection laws.	Compliance with Data Protection Laws: Continuous monitoring of changes in data protection laws to maintain compliance.
Inappropriate Content: Risk of exposure to inappropriate content or communication on the platform.	Monitoring and Moderation: The platform is monitored for inappropriate content, with swift action taken to address any issues.
Cloud-Based Storage of Personal Data, including Sensitive Information	Complies with the UK GDPR and Data Protection Act 2018, stipulating strong safeguards against unauthorised system access.
Transfer of Data between the School and the Cloud	Utilises advanced encryption measures as required by the UK's Information Commissioner's Office (ICO).
Geographical Location of Cloud Solution and Data Storage	Ensures data storage processes adhere to UK regulations, considering the UK's exit from the EU.
Cloud Service Provider's Commitments to Privacy and the Rights of Data Subjects	Respects the rights of data subjects as outlined in the UK GDPR and Data Protection Act 2018.
Implementation of Data Retention in the Cloud	Aligns data retention policies with UK GDPR requirements and guidance provided by the UK's ICO.
Response to a Data Breach	Follows the ICO's recommended procedures in case of a data breach, including notifying the ICO within 72 hours.
Transfer of Personal Data outside the UK	Complies with the ICO's guidance on international transfers and uses appropriate safeguards as per UK GDPR when transferring data.
Subject Access Requests	Complies with subject access requests as per the UK GDPR, including provision of data in a structured, commonly used format.
Data Ownership	Complies with principles of data controllership and processing as outlined in the UK GDPR and Data Protection Act 2018.
Cloud Architecture	Recommends regular review of cloud technologies used to ensure alignment with latest guidance from the ICO and other UK regulations.
GDPR Training	Ensures staff receive training tailored to the UK GDPR and Data Protection Act 2018.
Back up of Data	Follows best practice guidance on data backup from the ICO and the National Cyber Security Centre (NCSC).

Security of Privacy	Adheres to the principles of the UK's Data Protection Act 2018 and the ICO's guidance, ensuring strong security measures.

Summary

In conclusion, ClassDojo's DPIA highlights its conscientious approach to data handling practices. The platform collects and processes minimal necessary data to provide a personalised and efficient educational experience. While acknowledging potential risks such as data breaches, misuse of data, non-compliance with data protection laws, and exposure to inappropriate content, ClassDojo has implemented robust security measures and operational protocols. These include encryption, firewalls, regular staff training, compliance monitoring, third-party audits, user controls over personal data, and strict content moderation. This DPIA serves as a testament to ClassDojo's commitment to the privacy and security of its users, it should be reviewed and updated to reflect changes in data handling practices and regulations.

Decision

As a school, we have a responsibility to provide the best possible education and to create an environment that facilitates effective learning. Part of this responsibility involves using technology to enhance student learning experiences, communication between teachers and students, as well as managing student behaviour. ClassDojo is one such technology that supports us in these tasks, particularly because of its unique offerings which include classroom management, instant messaging, and progress tracking.

The decision to use ClassDojo is driven by the 'legitimate interests' clause of the General Data Protection Regulation (GDPR). Under Article 6(1)(f) of the GDPR, the school has the legal basis to process personal data if it's necessary for the purposes of the legitimate interests pursued by the school or a third party, unless these interests are overridden by the individual's interests or fundamental rights and freedoms which require protection of personal data.

Our legitimate interests in using ClassDojo are:

- Educational Interest: Enhancing the learning experience and improving the educational outcomes for students.

- Operational Efficiency: Streamlining communication between teachers, students, and parents.

- Behaviour Management: Helping teachers manage student behaviour effectively to maintain an ideal learning environment.

- Progress Tracking: Providing real-time tracking of student progress for teachers and parents.

The rights and freedoms of individuals have been taken into account in this decision. ClassDojo has a robust data protection and security infrastructure in place, which meets GDPR requirements and the UK's Data Protection Act 2018, to safeguard the data of users. It employs strong security measures such as encryption, firewalls, and secure socket layer (SSL) technology, and complies with stringent data minimisation principles.

Moreover, ClassDojo adheres to UK GDPR requirements on data retention, data transfer outside the UK, and provides parents and students with rights such as the right to access, rectify or delete their data, as well as to object to the processing of their data.

Therefore, given these robust data protection and privacy measures, and in balancing the rights and freedoms of individuals with our legitimate interests, we deem it reasonable to use ClassDojo without explicit parental consent. Parents will, however, be informed about the use of ClassDojo and our reasoning behind this decision to ensure transparency. They will also be given the option to discuss any concerns they may have.

It should be noted that if there are cases where we process special category data (e.g., information about health, race, or religion) using ClassDojo, we will always seek explicit consent as required by data protection laws.