Data Protection Impact Assessment

Google Classroom

Name of School: BOUNDS GREEN INFANT & JUNIOR FEDERATED SCHOOLS

Assessment Carried Out By: School Business Services and Senior Leadership Team

Reviewed By DPO On: 17-11-2020

Name and Aim of Project/Technology/System
Google Classroom (Learning Management System) G Suite for Education. Google Classroom is a free web service developed by Google and part of the G suite for Education to help schools streamline the process of sharing files between teachers and students. Students using Google Classroom can view assignments submit homework, and receive grades from teachers to help them stay on track and organised https://edu.google.com/products/classroom/?modal_active=none
Personal Data Used by Project/Technology/Sytem
Collection or use of data is limited to product requirement. Name, email address and password, DOB Information from google services - device information, log information, cookies.
Purpose of Processing
The school will rely upon its public task in the education of its students as a fair reason for processing. Opt-in consent is provided by parents of students or students over 12 years of age.

Steps taken to protect data

Steps Google will take to protect data

- Account creation is required.
- Two factor account protection is available.
- Third party contractual security protections are required.
- Industry best practices are used to protect data.
- All data in transit is encrypted.
- All data at rest is encrypted.
- Notice is provided by Google in the event of a data breach.
- Opt-in consent is requested from users at the time personal information is collected.

Google are fully committed to the security and privacy of data and protecting the school from attempts to compromise it. Google's systems are among the industry's most secure and they resist any unlawful attempt to access customers' data.

Google's data centres use custom hardware running a custom hardened operating system and file system. As Google controls the entire hardware stack, they are able to respond to any weaknesses or threats which may emerge.

In order to reaffirm the commitments Google has made to schools, Google has signed the Student Privacy Pledge. This pledge, introduced by the Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA), is intended to reflect their commitment to safeguard student personal information in their services designed for use in schools.

In the event of a possible data breach by Google, Google will notify the school or will guide them know what other security measures to put in place to stay better protected.

Data is shared with third party service providers. Contractual limits are placed on third-party data use.

Data is shared for analytics and research and/or product improvement

Data retention:

Google provides an option for the School to delete this data 3 months or 18 months after which the information is automatically deleted. Please outline which option the School is going to adopt.

School Security Features

- The school has a remote learning policy in place.
- The Senior Leadership will set clear protocols on use of Google Classroom
- The school has safeguarding protocols in place
- The School uses LGFL for their ISP provider, which has a strong router rules for safeguarding. The router filters external incoming traffic into the school network and blocks traffic, sites that are improper for education settings.
- The school also has IMPERO. IMPERO is a child safe guarding software that monitors both external and internal traffic to the school. It also monitors key word searches that are improper or flagged up as a point of concern. When this happens, it takes note of the student or staff also a snap shot of the key word that has triggered the alert and email it to the safeguarding lead in the school for further investigations.
- Staff and students within the network are also limited by their user accounts as to what documents and folders they have access to. Documents and folders are protected by

security access level and cannot be assessed by a staff of students who does not belong to that security group. Pupils will have limited access to only see what is necessary.
- The same is mirrored to their Gmail accounts. When a staff or student logs on using their Gmail account they also belong to security groups that gives them permission or access only to documents they have access to. This complements the security and GDPR compliant security measures that Google has implemented to Gmail.
- This also secures the Gmail class room and virtual learning. A student can only access the portal for learning if only an account exists for that student in the organization as well as the student being given the permission to attend the online classes.
- The school also uses Sophos for antivirus protection. Sophos is configured for real time scanning and access as well within the school.
- Staff will receive regular training on Google Classroom which will include good practice. Teachers will be given dedicated time to set up and run online classes.
- Users must change their passwords regularly. User passwords are required to have a combination of upper and lower case letters, numbers and symbols
- Data is retained for 18 months on the portal.

Impact And Risks

School Assessment of Risk		
	Risk Level	**Comments**
Likelihood of harm to data subject	Unlikely	As above, we have rigorous security protocols in place
Severity of harm (regardless of likelihood)	Minimal	Will depend on level of data used over classrooms (for example is any health, safeguarding, SEN data used?)
Overall risk (taking into account measures to reduce risk above)	Low	
DPO Assessment of Risk		
Likelihood of harm to data subject	Unlikely	
Severity of harm (regardless of likelihood)	Minimal to Significant	If sensitive data is shared/discussed, the severity of harm would be heightened.
Overall risk (taking into account measures to reduce risk above)	Low	

Compliance Statement

I can confirm that this data protection impact assessment has been completed to the best of my knowledge and that the software complies with the data protection principles under the GDPR.

All privacy risks and solutions have been considered and represent a proportionate response to the identified risks to personal data.

Signed: **Date: 16th November 2020**

DPO Statement

I can confirm that I have reviewed the DPIA above and are satisfied that the school have taken appropriate and proportionate steps to protect the data **OR** I confirm that I have review the DPIA above and have made recommendations set out in the comments above which should be accounted for before implementing the above.

Signed: PP. JSuldecka for and on behalf of Judicium Consulting Ltd
Date: 17-11-2020

Judicium Education
Judicium Consulting Ltd
72 Cannon Street
London EC4N 6AE