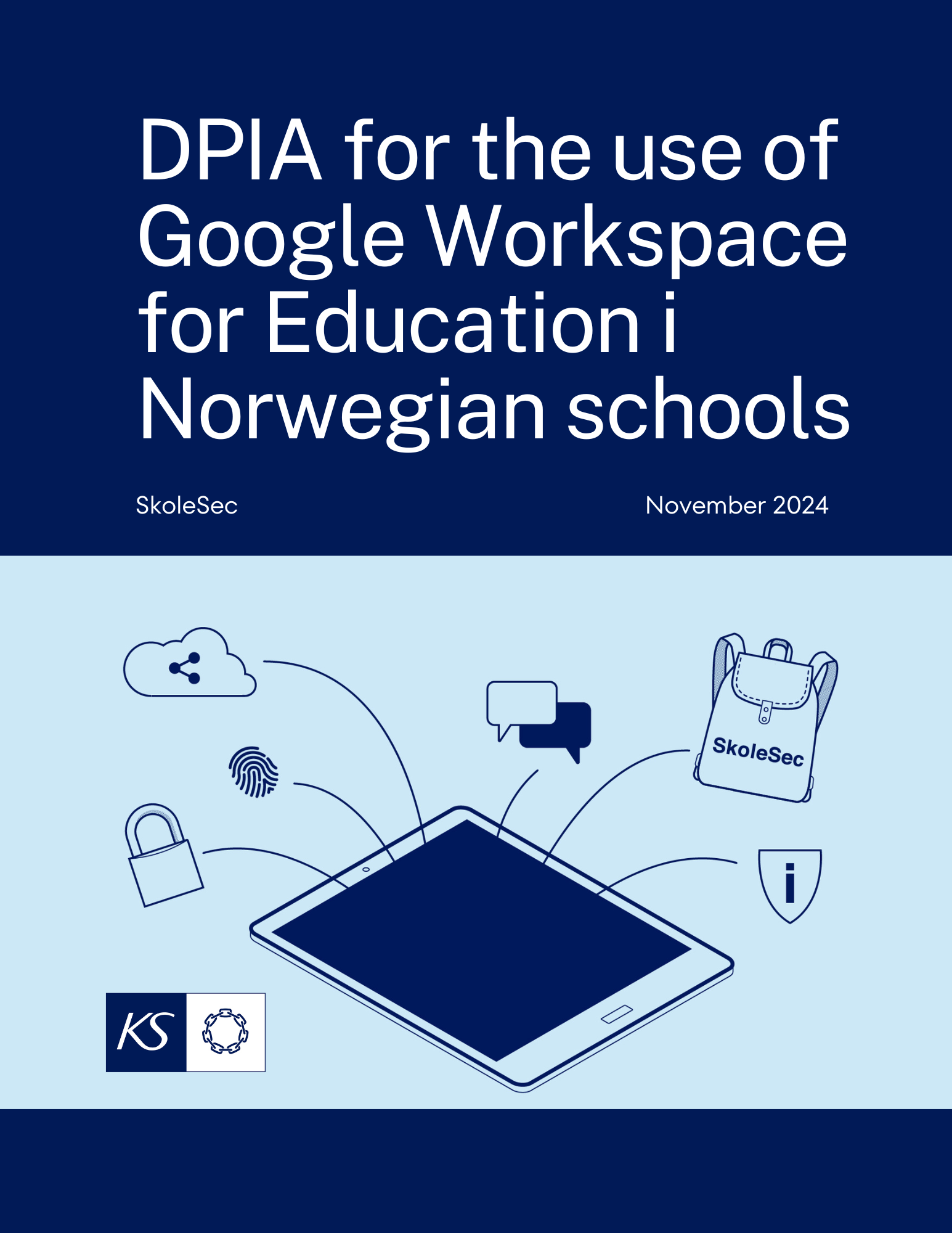
****

|  |  |  |  |
| --- | --- | --- | --- |
| Version Log | | | |
| Version | Date | Change | Author |
| 1.0 | November 2024 |  | KS, SkoleSec by Ida Thorsrud |
|  |  |  |  |

Disclaimer on the AI-assisted translation

This document has been translated from Norwegian to English using ChatGPT-4, an AI language model developed by OpenAI, in December 2024. While editorial adjustments have been made to improve clarity and readability, discrepancies from the original Norwegian text may still occur.

Table of contents

[Which Google Workspace for Education services should be used? 4](#_Toc185597840)

[Overview of services evaluated 6](#_Toc185597841)

[Roles and responsibilities 7](#_Toc185597842)

[Overview of who is the controller and who is the processor 7](#_Toc185597843)

[The legal basis for processing determines which digital services a municipality may use in a school setting 8](#_Toc185597844)

[Whether Google is the controller depends on the type of personal data involved, the services being used, and how they are used 8](#_Toc185597845)

[Processing activities, personal data, and legal basis for each processing 9](#_Toc185597846)

[School owners' processing of personal data 9](#_Toc185597847)

[Categorization of personal data processed by the school owner in Google Workspace for Education 10](#_Toc185597848)

[Processing activities 10](#_Toc185597849)

[Google’s processing of personal data 11](#_Toc185597850)

[Customer personal data 11](#_Toc185597851)

[Service data 11](#_Toc185597852)

[The school owner's purposes for processing personal data in Google Workspace for Education 12](#_Toc185597853)

[1. Promote learning and enable individualized and varied teaching 12](#_Toc185597854)

[2. Fulfill the school's duty of care to follow up on school environment cases 12](#_Toc185597855)

[3. Protect the solution, detect misuse, and prevent illegal activities 13](#_Toc185597856)

[4. Fulfill requirements for legally mandated disclosure of personal data 13](#_Toc185597857)

[Privacy principles 14](#_Toc185597858)

[This section describes how the school owner's processing of personal data in Google Workspace for Education complies with privacy principles. 14](#_Toc185597859)

[Is the requirement for lawfulness, fairness, and transparency upheld? 14](#_Toc185597860)

[Is the requirement for purpose limitation fulfilled? 16](#_Toc185597861)

[Is the requirement for data minimization fulfilled? 16](#_Toc185597862)

[Is the requirement for the accuracy of data fulfilled? 17](#_Toc185597863)

[Is the requirement for storage limitation fulfilled? 17](#_Toc185597864)

[Is the requirement for integrity and confidentiality fulfilled? 17](#_Toc185597865)

[Rights and freedoms of data subjects 18](#_Toc185597866)

[How is the data subject’s right to information upheld? 18](#_Toc185597867)

[How is the data subject’s right to access upheld? 18](#_Toc185597868)

[How is the data subject’s right to rectification upheld? 19](#_Toc185597869)

[How is the data subject’s right to erasure upheld? 19](#_Toc185597870)

[How is the data subject’s right to object upheld? 20](#_Toc185597871)

[How is the data subject’s right to restriction upheld? 20](#_Toc185597872)

[How is the data subject’s right to data portability upheld? 20](#_Toc185597873)

[How is the data subject’s right not to be subject to automated decision-making upheld? 20](#_Toc185597874)

[Summary of necessity and proportionality 20](#_Toc185597875)

[Qualitative Method 22](#_Toc185597876)

[The data subjects’ viewpoints 23](#_Toc185597877)

[Summary of the data subjects’ viewpoints and recommendations 23](#_Toc185597878)

[Recommendation from the Data Protection Officer 23](#_Toc185597879)

[Decision by the manager responsible for privacy 24](#_Toc185597880)

[Description of the factors considered by management in their decision: 24](#_Toc185597881)

[Appendix 1: Rationale for Recommended Services 25](#_Toc185597882)

[Appendix 2: Assessment of whether Google’s processing of personal data for its own purposes is compatible with the school owner’s original purposes under the Education Act 28](#_Toc185597887)

[Appendix 3: Overview of Agreements Governing Google Workspace for Education, ChromeOS, and Chrome Browser 31](#_Toc185597888)

[Appendix 4: Illustration of Recommendations 33](#_Toc185597893)

Recommendations

# Which Google Workspace for Education services should be used?

Regarding the use of Google Workspace for Education, our assessment is that Norwegian school owners may continue using the following services:

1. Google Workspace for Education (core services and AppSheet) when the school owner has accepted the supplementary agreement “Service Data Addendum”.[[1]](#footnote-2)
2. Chrome browser when the school owner has enabled “Data Processor Mode” (DPM)[[2]](#footnote-3) and uses it on a managed Chromebook.[[3]](#footnote-4)
3. «Essential Services»[[4]](#footnote-5) in ChromeOS when the school owner has enabled *“Data Processor Mode” (DPM)* [[5]](#footnote-6) and uses it on a managed Chromebook[[6]](#footnote-7)

The DPIA project recommends school owners not to use the following Google services::

1. Additional services in Google Workspace for Education.[[7]](#footnote-8)
2. Chrome browser when Data Processor Mode is not enabled.[[8]](#footnote-9)
3. Chrome browser when used on an unmanaged Chromebook.
4. “Optional services” in ChromeOS.[[9]](#footnote-10)

See Appendix 1 for the rationale behind recommended services. See Appendix 4 for an illustration of the recommendations.

|  |
| --- |
| The municipality is the school owner and controller for how students', teachers', and other staff's personal data is processed. In this DPIA, we provide several recommendations that the controller may choose to follow or not.  The recommendation regarding the additional services described above is one of them. If the controller chooses to continue using the additional services, we have written an article about measures the school owner should consider implementing.[[10]](#footnote-11) |

Del 1 Systematic description of processing activities

# Overview of services evaluated[[11]](#footnote-12)

This DPIA covers the processing of personal data in the following Google services:

* Core services in Google Workspace for Education
* Additional services *Google Search*, *Assistant*, and *YouTube*
* Chrome browser when used with a Google Workspace for Education account
* ChromeOS (the operating system on a Chromebook)

Et bilde som inneholder tekst, skjermbilde, diagram, Font

Automatisk generert beskrivelse

Figur 1 Overview of the services evaluated in this DPIA

**Brief description of Google Workspace for Education**

Google is a commercial company primarily known for its search engine "Google" and a range of services aimed at consumers. [[12]](#footnote-13) Google has also developed and adapted some of these services for the education sector in an office suite called *“Google Workspace for Education”*. While some of these services share the same names as consumer-market services, the services that are part of *Google Workspace for Education* are distinct from Google’s consumer services.

Google Workspace for Education is a cloud-based platform (SaaS) [[13]](#footnote-14) from Google Cloud, offering various tools and services for educational institutions. Google Workspace for Education targets school owners and has a business model different from Google’s consumer services.

Google Workspace for Education consists of “core services” and services categorized as *“other services” (AppSheet)*.[[14]](#footnote-15) School owners can also add other Google services to Google Workspace for Education, often called *“additional services”*.[[15]](#footnote-16)

* + - * 1. Core services

Core services are the foundational services in Google Workspace for Education. All users have access to these services. The municipality can decide which of these services students and teachers should have access to.[[16]](#footnote-17)

In principle, the municipality is the controller for the processing of personal data [[17]](#footnote-18) that occurs in Google Workspace for Education, while Google acts as a processor.[[18]](#footnote-19)

* + - * 1. Other services

Among the services in Google Workspace for Education, *“AppSheet”* is not defined as a core service but as *“other services”*. [[19]](#footnote-20) This is a web-based platform.

* + - * 1. Additional services

Additional services are services that the municipality must enable manually. They may incur additional costs, and the municipality must actively choose to use them before they can be implemented. These services are also tailored to the education sector, but Google, in addition to the school owner, is the controller for the processing of personal data that occurs in additional services.

The additional services YouTube and Google Search and Assistant are the two services evaluated in this DPIA. However, Google is the controller for all additional services. Thus, our recommendations regarding these additional services also apply to other similar services.

* + - * 1. Chrome services

This DPIA also considers the Chrome browser and ChromeOS, which is the operating system on a Chromebook. These products are not part of Google Workspace for Education, but they integrate well with other Google services. We have referred to these as “Chrome services”, and Google is generally the controller for the processing of personal data in Chrome and ChromeOS.[[20]](#footnote-21)

# Roles and responsibilities

## Overview of who is the controller and who is the processor

In Norway, the municipality as the school owner[[21]](#footnote-22) is the controller when students' personal data is processed in schools. This means that the school owner is responsible for ensuring students' privacy and the rights outlined in the GDPR are upheld.[[22]](#footnote-23) A controller determines why personal data is processed (the purpose of processing) and how it is processed by selecting the digital tools used to achieve this purpose.

The provider delivering digital services to the school owner is, in principle, a processor. A processor processes personal data on behalf of a controller. This means the processor cannot use personal data for other purposes than those instructed by the controller. This instruction is formalized through a “Data Processing Agreement” (DPA).

## The legal basis for processing determines which digital services a municipality may use in a school setting

As the controller, the school owner must have a legal basis to process students' personal data. This legal basis sets the framework for what the school owner can do with students' personal data. For example, the school owner cannot process students' personal data for purposes other than those stipulated in the Education Act.

This places limitations on the services that the school owner can procure from Google when Google acts as the controller.

For Norwegian school owners, the primary legal basis is GDPR Article 6(1)(e) (processing necessary for tasks carried out in the public interest),[[23]](#footnote-24) while the various provisions of the Education Act serve as the supplementary legal basis.[[24]](#footnote-25)

## Whether Google is the controller depends on the type of personal data involved, the services being used, and how they are used

The question of when Google is the controller and when it is the processor must be answered based on the type of personal data being processed ("customer personal data"[[25]](#footnote-26) or "service data"[[26]](#footnote-27)), the services being used,[[27]](#footnote-28) and also the type of operating system on which the services are used. [[28]](#footnote-29)

“Customer personal data” (also called “customer data”) is all information uploaded, stored, sent, or received in Google services. This includes, for example, the text of an assignment a student submits to a teacher, the written feedback the student receives from the teacher, or messages that students send to each other via Chat. Simplified, this can be described as “content data,” as opposed to “metadata.”

“Service data” (also called “service-related data”) is information collected or generated by Google as part of the use, delivery, and administration of the service. Somewhat imprecisely, this can be referred to as metadata. This is imprecise because “service data,” as defined in Google’s terms of use, also includes data that is not metadata, for example, information necessary for billing or user support (support tickets).

Metadata is also often referred to as diagnostic data. This is data that shows how a student or teacher uses Google Workspace for Education. This data is indirectly identifiable personal data. This means that it is personal data since it is possible for Google to identify individuals. However, the purpose is not to identify the individual student or teacher using Google Workspace for Education. The purpose is to obtain information about how the user base in general uses the services.

This means that the school owner must review the agreement that governs the specific services purchased in order to assess roles and responsibilities, namely when the school owner is the sole controller, when Google is the processor, and when Google is also the controller.

In summary, roles and responsibilities for Google Workspace for Education can be presented in the table below. Note that we have marked in red where Google’s role is not in line with the school owner’s responsibilities and the framework set by the Education Act.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Service** | **Controller** | | **Processor** | |
| *Customer personal data* | *Service Data* | *Customer personal data* | *Service Data* |
| Google Workspace for Education core services *without* Service Data Addendum | Municipality/ School owner | Google[[29]](#footnote-30) | Google | N/A |
| Google Workspace for Education core services *with* Service Data Addendum | Municipality/ School owner | Municipality/ School owner  Google (for the purposes set out in the Supplemental Google Cloud Privacy Notice)[[30]](#footnote-31) | Google | Google |
| YouTube (Google Workspace for Education additional service) | Google | Google | N/A | N/A |
| Google Search and Assistant (Google Workspace for Education additional service) | Google | Google | N/A | N/A |
| ChromeOS and Chrome browser with Data Processor Mode on managed Chromebook (ChromeOS essential services) | Municipality/ School owner | Municipality/ School owner  Google (for «legitimate business purposes»)[[31]](#footnote-32) | Google | Google |
| ChromeOS and Chrome browser with Data Processor Mode on managed Chromebook (ChromeOS optional services) | Municipality/ School owner Google | Google | Google | N/A |
| ChromeOS and Chrome browser without Data Processor Mode on managed Chromebook (ChromeOS) | Municipality/ School owner Google | Google | Google | N/A |

Table 1 Overview over who is a controller and who is a processor[[32]](#footnote-33)

# Processing activities, personal data, and legal basis for each processing

## School owners' processing of personal data[[33]](#footnote-34)

In this DPIA, we have focused on what, why, and how school owners process personal data of students and teachers, with primary focus on students. We have provided a systematic description of the processing activities taking place in schools. This means that we have concentrated on the activities themselves, i.e., how personal data is processed, rather than the system being used (here, Google Workspace for Education). However, the system’s functionality has also established boundaries for how personal data is actually processed.

Refer to the proposed record of processing activities for Google Workspace for Education, which is attached to this DPIA as an Excel file, for an overview of which personal data the school owner processes when Google Workspace for Education is used in schools, and the legal basis for each specific processing activity.

### Categorization of personal data processed by the school owner in Google Workspace for Education

* Identifiable information: name, email address, photo, username, phone number, address.
* Demographic information: school, class.
* Internet communication data: MAC address, IP address, cookies, location.
* Activities: behavioral patterns, login/logout times, submission times, times spent working on documents, times for chatting with friends.
* Free text: continuous text, submissions, communication content, special categories of personal data.
  + - * 1. Processing of special categories of personal data (free text)

In this DPIA, we have chosen to highlight that processing of what can potentially be special categories of personal data, as defined in GDPR Article 9, occurs in schools through teaching and classroom activities.[[34]](#footnote-35)

Special categories have been included in the category we refer to as free text. This is to clarify that the processing of special categories of personal data is not done by the school owner with the intention of processing this data. Google Workspace for Education contains multiple opportunities to enter free text, both when students write and submit assignments and during communication between student-student and student-teacher. In such free-text fields and in these types of communication channels, individuals may enter information about themselves or others that falls under special categories of personal data.

### Processing activities

We have chosen to divide the record of processing activities into different categories: pedagogical, administrative, and IT-technical. These groupings provide an indication that the processing activities may have different purposes and legal bases.

All activities collectively constitute the school owner's processing activities, clarifying the school owner's responsibilities, the provider's responsibilities, and the scope for processing personal data.

* + - * 1. Pedagogical activities
        2. Pedagogical activities include tasks such as distributing and submitting assignments, collaborative document editing, communication between teachers and students, and exams. These activities are carried out to “promote learning and enable individualized and varied teaching.” The primary legal basis is GDPR Article 6(1)(e), cf. Section 25-1 of the Education Act (processing personal data for necessary purposes), Section 11-1 (individualized teaching), and Section 2-3, fourth paragraph (teaching must be in accordance with the curriculum and facilitate active student participation).
        3. Administrative activities
        4. Administrative activities include tasks relevant to school administration, such as conducting exams, investigating school environment cases, and extracting data. The purposes and legal bases vary depending on the activity but generally involve addressing incidents, ensuring data quality, and maintaining a safe school environment.
        5. IT-technical activities

These activities ensure and monitor the use of services, manage tools and clients, and provide access and restrictions for students and staff. Here, too, the purpose can vary, but overall, the aim is to ensure the secure use of services by students and staff and to provide support and assistance. The legal basis is often a legal obligation (GDPR Article 6(1)(c)), based on GDPR Article 32(1) and Section 15(2) of the eGovernment Regulations (obligation to implement appropriate measures to achieve a good level of security).

## Google’s processing of personal data

### Customer personal data

When the school owner uses the core services in Google Workspace for Education or Chrome services with Data Processor Mode on a managed Chromebook, the school owner is solely the controller for “customer personal data.”[[35]](#footnote-36) This means that Google processes this personal data based on instructions from the school owner.

"Customer personal data" includes all information that is uploaded, stored, sent, or received in Google services and can be linked to an individual. For example, this includes the text of an assignment a student submits to a teacher, the written feedback the student receives from the teacher, or messages exchanged between students via Chat. In other words, this constitutes personal data. Simplified, it can be referred to as "content data," as opposed to "metadata."[[36]](#footnote-37)

### Service data

“Service data” is personal data that Google uses for its own purposes. In this case, Google acts as the controller for this type of personal data. This includes:[[37]](#footnote-38)

* **Account information**: Information that the school owner must provide to create user accounts for Google Workspace for Education. For students, teachers, and staff in Norwegian schools, this includes personal data such as usernames, names, contact details (email addresses and possibly phone numbers), and, if applicable, job titles.
* **Cloud payments and transactions**: Google stores information about fees, payments, and billing details. In this DPIA, no situations were identified where individual users with a school account in Google Workspace for Education could make such payments. It is assumed that if this category of service data contains personal data, it will primarily be contact information for municipal staff responsible for billing or acting as the customer contact.
* **Settings and configurations**: Google processes information about settings and configurations for Google Workspace for Education. For example, this includes the security settings enabled by the municipality. The personal data processed in this context primarily involves information about which administrator user made changes to the settings.
* **Direct communication between users and Google via GWFE:** If a student, teacher, or municipal employee with a Google Workspace for Education user account sends a technical support request to Google through the platform, Google retains this correspondence. These are direct user feedback, such as comments on the user experience or requests for technical support.
* **Personal data on how users use Google Workspace for Education or Chrome services:** [[38]](#footnote-39)Google processes personal data on how users interact with the solution, which primarily consists of metadata. Metadata, also referred to as diagnostic data, includes information on how a student, teacher, or municipal employee uses Google Workspace for Education. Examples include details on software errors, operational status, performance data, and data from the devices used to access GWFE, such as device identifiers and IP addresses. These data are indirectly identifiable personal data, meaning they qualify as personal data since Google can identify individuals. However, the purpose of Google’s processing is not to identify individual students, teachers, or employees using Google Workspace for Education. Instead, the purpose is to deliver the service, provide recommendations for optimal use to the school owner as a customer, and enhance the security and availability of the solution. [[39]](#footnote-40) For more details on the purpose and the Education Act’s framework for processing metadata, see Appendices 1 and 2.

# The school owner's purposes for processing personal data in Google Workspace for Education

When the school owner processes personal data in Google Workspace for Education, this is done for several purposes. Refer to the attached proposed record of processing activities in Excel format for an overview of the school owner's purposes and processing activities. These purposes can be summarized as follows:

1. **Promote learning and enable individualized and varied teaching**
2. **Fulfill the school's duty of care to follow up on school environment cases**
3. **Protect the solution,** [[40]](#footnote-41) **detect misuse and illegal activities**
4. **Fulfill requirements for legally mandated disclosure of personal data**

## ****1. Promote learning and enable individualized and varied teaching****

**The primary purpose of using Google Workspace for Education is to fulfill students' right to education as specified in the Education Act. This purpose is generally described as:**

**"Promote learning and enable individualized and varied teaching."**

**Under this primary purpose, there are several sub-purposes related to typical school activities and the functionality of Google Workspace for Education, as well as support purposes to ensure students and teachers can use the solution effectively:**

* **Ensure that students have a digital tool to be used for learning. This includes producing student work, submitting assignments, accessing files and documents, collaborating with others, and accessing exams.**
* **Ensure that teachers have a digital tool to aid in teaching, to be used for providing instruction. This includes a tool for sharing educational material and assignments, collaborating with others, and giving individualized feedback to students based on their work.**
* **Provide assistance and support to administrators and users of Google Workspace for Education.**

## ****2. Fulfill the school's duty of care to follow up on school environment cases****

**The school has a statutory duty of care, which requires that it promptly investigates any suspicion or knowledge that a student does not have a safe and good school environment. When the school owner uses a tool like Google Workspace for Education, where students can communicate with one another, this becomes an arena that forms part of the school environment.**

**This means that the school owner may need to investigate students’ activities in Google Workspace for Education, such as reviewing communications between students or within groups. Such activities could become part of a school environment case.**

## ****3. Protect the solution, detect misuse, and prevent illegal activities****

The school owner processes a range of personal data in Google Workspace for Education for security purposes. This includes ensuring the principles of confidentiality, availability, and integrity, as well as detecting and responding to misuse of the solution and illegal activities.

This purpose includes several sub-purposes**:**

* **Restricting students' access to harmful content on the internet and the use of school tools.**
* **Ensuring proper use of equipment and internet services by students and teachers, by implementing the school owner's guidelines and security policies for managed devices and school accounts.**
* **Detecting and addressing phishing, spam, malware, viruses, data breaches, password leaks, hacking, DDoS attacks, and other security-related incidents.**
* **Following up on potential misuse of services.**
* **Identifying liability for lost equipment.**
* **Managing access controls to ensure students and teachers have appropriate access. For example, ensuring students do not gain teacher-level permissions in Google Classroom.**
* **Identifying users to maintain the principle of integrity. For example, ensuring that the correct user is identified or determining who is collaborating and sharing information, or participating in classroom activities.**
* **Detecting cheating and following up on suspected cheating during exams and other tests.**

## ****4. Fulfill requirements for legally mandated disclosure of personal data****

In some cases, the school owner may be required to disclose personal data from systems such as Google Workspace for Education to third parties. This would involve legally mandated disclosure, where it is particularly important to reference a specific legal basis for processing.[[41]](#footnote-42) The purpose of this is to "fulfill requirements for legally mandated disclosure of personal data."

The most relevant obligation for the school owner is the right of access. Under GDPR Article 15, the data subject has the right to access their own personal data, and the school owner must fulfill this right when requested by the data subject.

Additionally, the school owner may be required to disclose personal data to the police when there is a court decision under the rules for search and seizure in the Criminal Procedure Act,[[42]](#footnote-43) or to the Office of the Auditor General in connection with audits or inspections.[[43]](#footnote-44)

Part 2 Necessity and Proportionality

* + - * 1. This section of the DPIA ensures that the choices made by the school owner regarding the use of Google Workspace for Education are reasonable in relation to the purposes of processing and that they comply with privacy principles and the rights of the data subjects. Sections that must be completed by the school owner are highlighted in yellow.

## Privacy principles

### This section describes how the school owner's processing of personal data in Google Workspace for Education complies with privacy principles.

### Is the requirement for lawfulness, fairness, and transparency upheld?[[44]](#footnote-45)

#### Lawfulness (legal basis)

##### The principle of lawfulness primarily concerns the requirement that the controller must have a legal basis for the processing of personal data.

##### Core services

The school owner may use platforms such as Google Workspace for Education based on GDPR Article 6(1)(e).[[45]](#footnote-46) This is because the use of such digital platforms is necessary to perform tasks in the public interest or exercise official authority. Schools are also obligated to provide tailored instruction to ensure that all students can utilize and develop their abilities.[[46]](#footnote-47)

##### Additional services

Google acts as the controller for the additional services in Google Workspace for Education. This means that Google processes personal data for its own purposes. Specifically, Google processes personal data about how students, teachers, and others use the solutions to further develop existing and new commercial services.

The Education Act establishes boundaries for what the school owner—and by extension, the processors the school owner procures services from—may use personal data for. In a letter dated September 20, 2024, the Ministry of Education stated the following:

*"The Ministry cannot see that the school owner is obligated under the Education Act to contribute to the development of private actors' products, either through the provisions on tailored instruction or through other provisions in the Education Act. In the Ministry’s opinion, the school owner is therefore not permitted to share students’ personal data with providers for this purpose."*

This means that Norwegian school owners do not have a legal basis to use the additional services in Google Workspace for Education, as doing so would involve sharing personal data with Google, which would then process it to develop a private actor's products and services. Furthermore, this implies that using the additional services in Google Workspace for Education does not meet the requirement for lawfulness.

#### Transparency

The principle of transparency requires that the controller is obligated to be aware of and inform students, parents, and staff about how personal data is processed, by whom, and in what roles.[[47]](#footnote-48)

Describe how the school owner informs students, parents, teachers, and other staff about how their personal data is processed in Google Workspace for Education.

After this DPIA is completed, privacy implications are assessed, and the municipality has prepared a record of processing activities, the school owner will have an overview of what personal data is processed and how it is handled in Google Workspace for Education.

We recommend that the school owner subsequently updates the information provided, for example, in the municipality’s privacy statement or on a dedicated information page on the internet.[[48]](#footnote-49)

#### Fairness

For processing to be fair, there must be a clear connection between the collection and use of personal data, and the processing should appear reasonable to the data subject.[[49]](#footnote-50)

##### Core services

Personal data in schools is primarily collected to provide each student with education in the present or to enable staff to teach and facilitate a positive school environment. Examples include distributing and submitting assignments. Processing personal data for these activities, such as names and class or group affiliations, appears predictable and reasonable for those concerned. The same applies to staff working in schools.

Processing of "service data," which is metadata (data about data) generated when students and staff use Google's tools, may seem less predictable, often because it is a less "visible" activity to the naked eye.

The DPIA project assesses that metadata processed for purposes such as delivering the service, providing recommendations for optimal use to the school owner as a customer, and ensuring and improving the solution's security and availability is particularly necessary to deliver the service. Furthermore, it is our assessment that the additional purposes are reasonable and predictable, as they uphold fundamental information security principles (confidentiality, integrity, and availability) and facilitate safe and efficient use of the solution by the school owner.

A secure and accessible service, for example, prevents unauthorized access to the service and shields students from harmful content. Often, it is natural and necessary for the school owner to delegate some of this processing to the service provider. This aligns with the school owner’s discretion to select the tool best suited to achieving the purpose of tailored education.

Google offers various agreements or "terms of service" for Google Workspace for Education, which allow for different arrangements regarding who is the controller for metadata. This means that Norwegian school owners must choose agreements where they retain the responsibility for metadata. Under these agreements, Google cannot use personal data for its own purposes unless the new purposes are compatible with those of the controller (providing quality education in a positive environment).

##### Additional services

Due to the conclusion regarding the additional services above, the requirement for fairness cannot be considered fulfilled concerning the additional services.

### Is the requirement for purpose limitation fulfilled?[[50]](#footnote-51)

##### Core services

The principle of purpose limitation stipulates that personal data must be "collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes."[[51]](#footnote-52)

The project has specifically outlined the purposes for each processing activity; see the attached record of processing activities. These purposes align with the main goal of the Education Act, which is to ensure that children and young people receive quality education in a positive environment,[[52]](#footnote-53) and with the fundamental requirement in the curriculum for digital skills.[[53]](#footnote-54) To provide digital tools for education, the school owner must also ensure the proper operation of their data systems in accordance with the KIT principles (confidentiality, integrity, and availability). These purposes are therefore legitimate based on the school owner's obligation to fulfill the right to primary education.[[54]](#footnote-55)

Further processing of personal data cannot occur in a manner incompatible with these purposes.[[55]](#footnote-56) As discussed under the fairness requirement above, the project has evaluated the further processing of metadata for the purposes of "delivery, availability, and security of the service." This purpose is often naturally delegated to the processor. We consider this purpose compatible with the school owner’s obligation to ensure the proper operation of data systems (KIT principles).[[56]](#footnote-57)

Further processing for "archival purposes in the public interest," in accordance with GDPR Article 89(1), is not incompatible with the original purpose.[[57]](#footnote-58) The school owner may therefore archive and document personal data in compliance with the Archival Act and its related regulations. However, it should be noted that office support solutions and school learning platforms like Google Workspace for Education are not suitable archival systems.

##### Additional services

The requirement for purpose limitation is not fulfilled for the additional services; see the assessment of lawfulness above.

### Is the requirement for data minimization fulfilled?[[58]](#footnote-59)

##### Core services

The principle of data minimization requires that processing must be "adequate, relevant, and limited to what is necessary for the purposes for which they are processed." In other words, no more personal data should be processed than necessary to achieve the purpose. This also involves assessing whether fewer data could be processed or whether measures such as pseudonymization or anonymization could be implemented.[[59]](#footnote-60)

In a school context, it can be challenging to process minimal data about students as long as the purpose is tied to pedagogical activities. This relates to one of the main objectives of education, which is to enable students to "develop creativity, engagement, and a desire to explore," cf. Section 1-3 of the Education Act. This means that students are expected to actively contribute to their education (§10-6).

Therefore, it is not the school owner's goal to limit the amount of content data (data created/shared by students and teachers) but rather to guide students based on the subjects and themes outlined in the curriculum. As a result, the amount of personal data in content data can be significant (see our discussion on Processing of special categories of personal data (free text) on page 10). Personal data related to students' active participation in education must be considered to have a close and natural connection to the purpose of the processing. Thus, the data are "adequate" and "relevant," while students themselves can limit the information they choose to provide.

For personal data associated with user accounts (e.g., logins), there is less flexibility in determining which data are "relevant" for processing. For user accounts, data identifying the student and the student’s class and school affiliation are the necessary personal data for this purpose.

For the processing of personal data for IT-related purposes, such as security, the aim is to meet the requirements for built-in privacy and the KIT principles (confidentiality, integrity, and availability). For instance, it will be necessary to process IP addresses and location data.

##### Additional services

The requirement for data minimization is not fulfilled for the additional services; see the assessment of lawfulness above.

### Is the requirement for the accuracy of data fulfilled?[[60]](#footnote-61)

The principle of accuracy requires that personal data must be correct and kept up to date. The school owner must ensure that personal data in Google Workspace for Education is accurate.

Personal data is kept up to date in Google Workspace for Education by pulling information about students, teachers, and other users from school administrative systems. Additionally, many personal data points come directly from the data subject, such as student work or communication between users.

Here, the school owner must describe any additional measures taken.

### Is the requirement for storage limitation fulfilled?[[61]](#footnote-62)

The school owner must evaluate documentation and archival obligations in accordance with the Directorate for Cultural Heritage’s regulation § 7-28, paragraph (3) on primary education. For example, "ongoing assessments, including semester evaluations with grades," must be archived in an appropriate archival and documentation system. Normally, student and employee user accounts (logins in GWFE via FEIDE accounts) are deactivated and deleted within a specific time frame after leaving the school. The school owner must conduct a specific assessment of how long it is necessary to retain the user account.[[62]](#footnote-63)

### Is the requirement for integrity and confidentiality fulfilled?[[63]](#footnote-64)

Refer to the explanations on how integrity, confidentiality, and other information security requirements are addressed in the attached overview of risk scenarios and the record of processing activities.

The school owner must describe any additional measures taken. Descriptions that could improve this section include:

* Technical role-based access control.
* Organizational measures, such as restricted access management based on operational needs.
* Limitations introduced by the school owner in Google Workspace for Education, such as restrictions on chat functionality.
* Established routines governing external sharing and collaboration with third parties.
* Procedures and requirements for investigating school environment cases, including students’ right to rebuttal.
* Alerts and follow-up routines when teachers accidentally grant students teacher-level access.
* Other relevant measures...

Remember: The school owner must complete both the record of processing activities and detail the technical and organizational security measures implemented. They must also evaluate the risk scenarios in the attached assessment (Part 3 of this DPIA) and describe additional risk scenarios relevant to their institution.

## Rights and freedoms of data subjects

This section describes how the school owner’s processing of personal data in Google Workspace for Education safeguards the rights and freedoms of data subjects.

### How is the data subject’s right to information upheld?[[64]](#footnote-65)

The right to information means that the school owner is obligated to inform students, parents, teachers, and other staff using Google Workspace for Education about how their personal data is processed.

Processing personal data, particularly in systems provided by large technology companies, is something many find difficult to understand. This applies both to citizens and school owners. As mentioned earlier, this project has found it challenging to fully comprehend Google’s service portfolio. Nevertheless, the school owner is responsible for understanding the purchased product and conveying information about its use to students, parents, and staff.

In this project, we have worked on clarifying legal questions, terms, and the distinctions between Google’s services, which we believe will help school owners better understand and manage Google Workspace for Education.

The school owner should, as a minimum, inform students and parents about which Google tools the municipality uses, what data about students is processed in the service, for what purpose, how long the data is stored, and the rights of the students. This can be communicated, for example, in a dedicated informational document or on the municipality’s website.

The school owner must explain how information about Google Workspace for Education is provided to students, parents, teachers, and other staff using the solution.[[65]](#footnote-66)

### How is the data subject’s right to access upheld?[[66]](#footnote-67)

The right to access gives students (and parents on behalf of students), teachers, and other staff the right to see what personal data is being processed about them in Google Workspace for Education.

Login to Google Workspace for Education is done through a Feide account. Students and staff can log in to Feide’s website to access all information stored in their digital user account. Schoolwork and assessments will be accessible to students and staff via their own PC or Chromebook.

Google Workspace for Education includes functionality that enables the school owner to fulfill the right to access. This is achieved both by allowing the data subject to download their own documents and by enabling the user to download their personal data via the Takeout feature.[[67]](#footnote-68),[[68]](#footnote-69)

The school owner must explain how students, parents, teachers, and other staff can exercise their right to access. There should be a designated contact point, either at the school or centrally, that can be contacted if assistance is needed to exercise the right to access. The school owner must also decide whether students who have completed their schooling should be given the opportunity to transfer their documents and files from their school account to a private Google account.

### How is the data subject’s right to rectification upheld?[[69]](#footnote-70)

Data subjects have the right to have inaccurate personal data about themselves corrected. This right must be understood in connection with the principle of accuracy, which obligates the school owner to ensure that the personal data processed in Google Workspace for Education is accurate and up to date.

Most of the personal data processed in Google Workspace for Education is either retrieved from the school owner’s administrative systems or created by the data subject themselves (e.g., student work or communication between users). As such, requests for rectification based on a data subject's inquiry will rarely be relevant.

The school owner must explain how students, parents, teachers, and other staff can exercise their right to rectification. There should be a designated contact point, either at the school or centrally, that can be contacted if assistance is needed to exercise the right to rectification. This contact point can also handle requests for deletion from data subjects whose personal data is processed by the municipality. The school owner must also inform users of Google Workspace for Education about how they can exercise this right.

### How is the data subject’s right to erasure upheld?[[70]](#footnote-71)

Data subjects have the right to have their personal data erased. This right must be considered in connection with the school owner's obligation for storage limitation, which requires the school owner to delete personal data from Google Workspace for Education once the purpose of the processing has been fulfilled.

For personal data processed in Google Workspace for Education, the school owner generally has a legal basis for processing the data subject's personal information. Therefore, requests for erasure based on inquiries from data subjects will rarely be applicable.

The school owner must explain how students, parents, teachers, and other staff can exercise their right to erasure. There should be a designated contact point, either at the school or centrally, that can be contacted if assistance is needed to exercise the right to erasure. This contact point can also handle other deletion requests from data subjects whose personal data is processed by the municipality.

The school owner must also inform users of Google Workspace for Education about how they can exercise this right. It should be noted that the right to erasure does not necessarily mean that the data subject has the right to have their personal data deleted, as the school owner generally has a legal basis for processing the personal data of students, teachers, and other staff in Google Workspace for Education.

### How is the data subject’s right to object upheld?[[71]](#footnote-72)

The right to object, as outlined in GDPR Article 21, applies to processing activities in schools that are based on GDPR Article 6(1)(e), "public authority or task carried out in the public interest," or (f), "legitimate interest." Most processing activities related to educational purposes are grounded in Article 6(1)(e), which means that students and parents have the right to lodge an objection.

The individual lodging an objection must point to reasons related to their specific situation. In other words, there must be individual circumstances that justify stopping the processing.

The school owner must explain how they are prepared to receive and process objections. This is a responsibility that many school owners may find challenging. To assist with this, we have prepared a guide for the right to object, which can help municipalities manage this right effectively: [Guide to the Right to Object – KS.](https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/veileder-for-retten-til-a-protestere/).

For both the right to object and the right to restriction, the school owner should have a designated contact point, either at the school or centrally, that students, parents, and staff can contact if they wish to exercise their rights.

### How is the data subject’s right to restriction upheld?[[72]](#footnote-73)

The right to restriction is a relevant right in connection with the right to object. See the explanation above regarding how the right to object is upheld.

### How is the data subject’s right to data portability upheld?[[73]](#footnote-74)

The right to data portability only applies when the legal basis for processing is consent or contract. The legal basis for using Google Workspace for Education is GDPR Article 6(1)(e), "public authority or task carried out in the public interest," with supplementary legal bases in the Education Act. Therefore, this right is not applicable.

### How is the data subject’s right not to be subject to automated decision-making upheld?[[74]](#footnote-75)

The core services in Google Workspace for Education do not include functionality that could be used to make automated decisions. Therefore, this right is not applicable.

## Summary of necessity and proportionality

Is the processing of personal data the least intrusive way to achieve the purpose?  
  
☐ Yes ☐ No

Explanation:   
[Insert explanation for the selection above. Why is the processing the least intrusive way to achieve the purpose? Why is the processing not the least intrusive way to achieve the purpose? Remember to highlight what changes can be made to achieve the purpose in a less intrusive manner, if applicable.]

Part 3 Assessment of Privacy Risks and Mitigation Measures

This section of the DPIA focuses on evaluating the privacy risks associated with the processing of personal data. For this DPIA, this has been done in a dedicated Excel sheet attached to the DPIA. Refer to this Excel sheet for the assessment of privacy risks and mitigation measures.

The school owner must assess and consider each risk scenario and add new ones relevant to the school owner’s local context.

# Qualitative Method

A qualitative method has been chosen for assessing privacy risks in this DPIA.

Traditional risk assessment models, such as various multi-factor models that evaluate the likelihood of a risk scenario occurring and its consequences, are often used in information security. However, such models may be insufficient for privacy risk assessments because they do not adequately account for internal factors that could lead to non-compliance with privacy principles and data subjects’ rights. The causes of such violations are often internal factors within the controller rather than external threats.

To address these challenges, a qualitative approach has been used for privacy risk assessments in this DPIA. This approach is based on professional judgment and contextual understanding, assessing risks at the following levels:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Risk level** | **Explanation** | **Example** |
|  | Low | There is no violation or significant risk of violating a principle, right, or freedom. | The processing is based on consent as the legal basis, but the language used to provide information about the consent is slightly unclear yet understandable. |
|  | Medium | There is a risk that a principle, right, or freedom may be violated or not always adhered to. | There may be a breach of data minimization if a free-text field lacks guidance text, making it likely that some users will enter more personal data than necessary. |
|  | High | It is evident that a principle, right, or freedom may be violated. | An older school administrative system is used for processing personal data, where deletion of data is not possible. |

Part 4 The Data Subject's Opinion and Advice from the Data Protection Officer

# The data subjects’ viewpoints

The viewpoints of the data subjects were gathered in connection with the completion of this DPIA. Refer to the reports on the opinions of students, teachers, and parents regarding privacy in Google Workspace for Education for detailed information about the privacy concerns of the data subjects.[[75]](#footnote-76)

# Summary of the data subjects’ viewpoints and recommendations

[Insert the participants' recommendations. Be sure to indicate whether the participants believe there is a high risk or not. Also include whether the participants think it is necessary to conduct a prior consultation with the Data Protection Authority / Supervisory Authority based on their understanding of the risk landscape.]

# Recommendation from the Data Protection Officer

[Insert the DPO’s comments on the DPIA.]

Part 5 Management’s Decision

# Decision by the manager responsible for privacy

The management’s decision after completing the privacy impact assessment is as follows:

The risk to the data subjects' rights and freedoms has been reduced to an acceptable level. Once measures are implemented, the processing of personal data can proceed.

The risk to the data subjects' rights and freedoms has not been reduced to an acceptable level. The processing of personal data cannot proceed.

The risk to the data subjects' rights and freedoms has not been reduced to an acceptable level. Prior consultation with the Data Protection Authority / Supervisory Authority will be conducted before management decides on the processing of personal data.

# Description of the factors considered by management in their decision:

[Insert the rationale for the decision made above.]

|  |  |  |
| --- | --- | --- |
| Date | Name of decision-maker | Role |
|  |  |  |

# Appendix 1: Rationale for Recommended Services

***Note that this document describes YouTube and Google Search and Assistant as services within Google Workspace for Education. YouTube and Google Search also exist as consumer services. What is described in this document does not apply to these services in their consumer form.***

## The school owner is the controller and must instruct providers on how students’ personal data should be processed

The school owner[[76]](#footnote-77) is the controller when students' personal data is processed in the school. This means the school owner is responsible for safeguarding students' privacy and the rights outlined in the General Data Protection Regulation (GDPR).[[77]](#footnote-78) A controller also determines why personal data is processed (the purpose of the processing) and how it is processed by selecting the digital tools necessary to achieve the purpose.

The provider delivering digital services to the school owner acts as a processor. A processor processes personal data on behalf of a controller. This means the processor cannot use the personal data for purposes other than those instructed by the controller. This instruction is referred to as a "data processing agreement."

Et bilde som inneholder tekst, skjermbilde, diagram, Font

Automatisk generert beskrivelse

*Figure 1 Google’s role as processor and controller defines the boundaries for services recommended for use by the school owner (within the green area) and services not recommended (within the red area)*

Part of the responsibility as a controller is to ensure that agreements are not made with processors who process personal data for "their own purposes." In other words, the controller must ensure that the processor only processes personal data in accordance with the instructions and the agreement. If a processor processes personal data for its own purposes, its status changes from processor to controller. In such a case, the processor (now acting as a controller) decides independently how to use the personal data. This situation is particularly problematic when it involves students' personal data, as it can be likened to "selling" students' personal data to the provider.

Many large providers do not negotiate their own data processing agreements with customers but instead use standard agreements. This is also true for Google. In the contractual framework underlying Google Workspace for Education, Google has outlined that they act as a controller for the additional services. This role distribution is incompatible with the school owner's responsibility as a controller.

## The school owner's legal basis determines which digital services can be used in schools

As the controller, the school owner must have a legal basis (a processing basis) to process students' personal data. For Norwegian school owners, the legal basis is provided by the various provisions of the Education Act. This legal basis sets the framework for what the school owner can do with students' personal data. For instance, the school owner cannot process students' personal data for purposes other than those specified in the Education Act.

This also limits which personal data the school owner can share with providers such as Google for their further use of students' personal data for their own purposes.

## The Education Act sets clear boundaries for what students' personal data (including metadata) can be used for

Although Google acts as a processor for the core services in Google Workspace for Education and for the Chrome browser when used on a managed Chromebook (ChromeOS), Google is always the controller for metadata.[[78]](#footnote-79)

Metadata is information about information—that is, data about how students and teachers use Google Workspace for Education. Examples of metadata include information about the wireless network a student’s Chromebook is connected to, the time the student logged into Google Classroom, or the version of the Chrome browser being used. Metadata is often referred to as diagnostic data or telemetry.

Metadata is distinct from content data. Content data includes, for example, the text of an assignment a student submits to the teacher, the written feedback the student receives from the teacher, or messages exchanged between students within the platform.

Metadata is indirectly identifiable personal data. Although Google can identify individual students, identification is not the purpose of Google’s processing of this data.[[79]](#footnote-80)

Most providers use this type of personal data (metadata) from their customers for their own purposes to varying degrees. Google is not unique in this regard. This issue was central to the Danish Chromebook case, where the Danish Data Protection Authority prohibited Helsingør from using Google Workspace for Education in 2022. In this case, the Danish Data Protection Authority determined that the Danish Education Act allowed personal data in Google Workspace for Education to be processed for the purpose of:

*Delivery, availability, and security of the service.*

However, the following purposes were deemed outside the scope of the Danish Education Act:

* *Further development of the specific service purchased by the school owner.*
* *Development of other and new products by the provider.*

The question of whether providers can use students' personal data for their own purposes has long been unclear. In September 2024, the Ministry of Education provided clarification that the Education Act does not permit the use of students' personal data for the development of private actors' products. The Ministry emphasized that this also means school owners cannot share students' personal data with providers for this purpose. Specifically, the Ministry stated:[[80]](#footnote-81)

*"The Ministry cannot see that the Education Act imposes any obligations on school owners to contribute to the development of private actors' products, either through the provisions on tailored instruction or through other provisions in the Education Act. In the Ministry’s opinion, school owners therefore cannot share students’ personal data with providers for this purpose."*

This means that the purposes for which the Education Act permits a provider to process student data are very limited. It is our assessment that the Norwegian Education Act allows Google and other providers to use students’ personal data for the following purposes:[[81]](#footnote-82)

*Delivery, availability, and security of the service, including further development of the service’s security and availability.*

The Education Act does not permit Google or other providers to process students’ personal data for the following purposes:

* Further development of the specific service purchased by the school owner.
* Development of other and new products by the provider.

## What are the probable and significant risks and consequences for students if schools continue to use Google Search, Assistant, and YouTube?

If school owners continue to use additional services such as Google Search, Assistant, and YouTube, there is a risk that they are disclosing students’ personal data to a commercial entity that then uses the data for purposes not aligned with the objectives outlined in the Education Act. The Ministry of Education’s statement from September 2024 has made this even clearer than before.

Google acts as the controller for all personal data processed in the additional services. This means Google can process students' personal data for its own purposes. This poses a privacy risk to students, as their personal data could potentially be further processed in ways that are not compatible with the Education Act. It also creates a compliance risk for school owners, as they fail to fulfill their responsibilities as controllers by allowing processing that does not align with their obligations under the law.

Google has implemented several measures to limit the personal data it collects about students.[[82]](#footnote-83) However, Google still collects personal data about students when they use additional services through a school account and uses this data for its own purposes.

# Appendix 2: Assessment of whether Google’s processing of personal data for its own purposes is compatible with the school owner’s original purposes under the Education Act

The school owner may process personal data when it is necessary to perform tasks under the Education Act, cf. Section 25-1 of the Education Act.

The Ministry of Education has previously concluded that there is no specific legal obligation in the Education Act to use Google Workspace for Education or similar software in schools.[[83]](#footnote-84)

The school owner, however, has a legal obligation to fulfill the right to primary and secondary education, cf. Sections 28-1 and 28-2 of the Education Act (2023). Furthermore, the Regulation on Overarching Goals and Principles in Schools (Overarching Part – Values and Principles for Basic Education), Section 2.3, defines digital skills as one of the five basic skills, requiring schools to facilitate and support students’ development of these skills throughout their education.

The Ministry considers these obligations sufficient to establish a legal requirement for school owners to adopt solutions such as Google Workspace for Education. The legal basis for using systems like Google Workspace for Education is thus GDPR Article 6(1)(e), cf. Section 25-1 of the Education Act, in conjunction with Sections 28-1 and 28-2, and the requirement for digital skills outlined in the Regulation on Overarching Goals and Principles in Schools, Section 2.3.

In other words, the Education Act and its regulations provide the legal framework for using solutions like Google Workspace for Education. This means that students’, teachers’, and other employees’ personal data may be used for purposes necessary to deliver the service. Google processes students' personal data to deliver the service. In this DPIA, we have defined this purpose as: "delivery, availability, and security of the service."

In Google Workspace for Education (core services and AppSheet), Google further processes students' personal data to "further develop the security and availability of the service."[[84]](#footnote-85) In the Chrome browser and in ChromeOS "Essential services" with Data Processor Mode, Google processes students' personal data for "improvement and optimization of performance and core functionality related to the effectiveness of availability, privacy, security, and IT infrastructure of the services."[[85]](#footnote-86)

*The question is whether this purpose is compatible with the original purpose of delivering the service.*

To assess this compatibility, we have used the Norwegian Data Protection Authority’s guidance on the principle of purpose limitation.[[86]](#footnote-87)

1. **Is there a natural connection between the original purpose and the new purpose?**

The original purpose of processing personal data is to use Google Workspace for Education as a tool to meet the requirements of the Education Act, particularly concerning the development of students' digital skills. The new purpose is to process students' personal data in the form of "service data" to further develop the security and availability of the service.

There is a natural connection between these purposes, as improving the service's security and uptime (availability) is a prerequisite for delivering the solution. Google Workspace for Education is a SaaS (Software as a Service) platform, and this type of service requires continuous development of security and availability to address technological advancements, respond to emerging security threats, and ensure that the service remains stable and reliable for users.

This supports the view that processing personal data to improve the service in the areas of "security" and "availability" is compatible with the original purpose. Since service improvement is essential for providing a safe and effective learning platform, it can be considered an extension of the original purpose and, therefore, in line with the principle of purpose limitation.

1. **In what context were personal data collected for the original purpose?**

The personal data were collected to facilitate the use of Google Workspace for Education within an educational context. This includes enabling students, teachers, and other staff to use Google Workspace for Education as part of the teaching and learning process. The data were gathered to support communication, collaboration, and access to learning resources, in alignment with the school’s obligations to develop students’ digital skills.

1. **What is the relationship between the controller and the data subject? Is the data subject part of a particularly vulnerable group or dependent on the controller?**

The data subjects are primarily school students, i.e., minors, who constitute a vulnerable group under the GDPR. Their age contributes to an asymmetric power dynamic between the data subjects and the controller.

This asymmetry is exacerbated by the fact that students have no choice about whether their personal data are processed in Google Workspace for Education. This decision is made on their behalf by the school owner (the municipality).

This situation places an added responsibility on the school owner to ensure that students’ personal data are processed in a manner that respects and safeguards their privacy.

1. **Is the new purpose and the processor's processing of personal data predictable for the data subject?**

As noted in question 1, there is a natural connection between the purpose of "further developing security and availability of the service" and the original purpose for which the personal data were collected. For the school owner, as the controller and professional customer of various digital services, it is predictable that personal data would be used for this purpose. However, this may not be as obvious to the data subjects (students and teachers using Google Workspace for Education).

Therefore, it is important to communicate this clearly to the data subjects, for example, through the municipality's privacy statement and information provided by the school. Transparency is essential to ensure that the processing is predictable and aligns with the data subjects’ reasonable expectations.

1. **Does the processing involve special categories of personal data?**

The processing does not involve special categories of personal data.[[87]](#footnote-88)

1. **Does the new processing of personal data pose specific risks to the data subject?**

The new processing is assessed not to pose specific risks to the data subject. This is because the new purpose is closely related to the original purpose, and the processing occurs within the same context and with comparable security measures. As a result, the new processing does not present particular risks to the data subject.

1. **Is it possible to implement special protective measures or necessary safeguards to protect the data subject's privacy, such as through pseudonymization?**

It is both possible and necessary to implement protective measures to safeguard privacy. In this case, measures have been implemented by collecting indirectly identifiable personal data. While the data are not directly pseudonymized, the collection of indirectly identifiable information reduces the risk of individuals being directly identified.

Additionally, Google has implemented various forms of encryption in the core services, which further protect the data subject’s privacy, particularly in terms of confidentiality.[[88]](#footnote-89)

**Conclusion**

This assessment shows that the processing of students’ activity data in the form of metadata ("service data") to ensure security and availability in Google Workspace for Education (core services and AppSheet), as well as in the Chrome browser and ChromeOS "Essential services" with Data Processor Mode, is compatible with the purpose of "further developing security and availability of the service."

This is because there is a natural connection between the original purpose of delivering the service and the new purpose of improving security and availability. Such further processing is necessary to provide a stable and secure learning platform.

# Appendix 3: Overview of Agreements Governing Google Workspace for Education, ChromeOS, and Chrome Browser

# **Google Workspace for Education core services and AppSheet**

1. Google Workspace for Education Privacy Notice: <https://workspace.google.com/intl/no/terms/education_privacy/>
2. Google Workspace for Education Terms of Service​: <https://workspace.google.com/terms/education_terms/>
3. Google Data Processing Addendum: <https://cloud.google.com/terms/data-processing-addendum/>
4. Google Cloud Privacy Notice: <https://cloud.google.com/terms/cloud-privacy-notice>
5. Cloud Data Processing Addendum: <https://cloud.google.com/terms/data-processing-addendum/>
6. Optional agreements we recommend you sign:
   * Google Workspace for Education Service Data Addendum: <https://workspace.google.com/terms/service-data-addendum/>

When the school owner has signed this document, the privacy statement will become this document: Supplemental Google Cloud Privacy Notice: <https://cloud.google.com/terms/cloud-privacy-notice-supplement>

# **Google Workspace for Education additional services**

YouTube

* Workspace for Eduaction Privacy Policy: <https://workspace.google.com/intl/no/terms/education_privacy/>
* Google Privacy Policy: <https://policies.google.com/privacy?hl=no>

Google Search and Assist

* Google Privacy Policy: <https://policies.google.com/privacy?hl=no>

# **Chrome services**

ChromeOS and Chrome browser (on a managed Chromebook with Data Processor Mode)

* ChromeOS Data Processor Mode Agreement: <https://www.google.com/chrome/dpchromeos/eu/index.html>

# What you need to know about the different agreements

The Google Workspace for Education Privacy Notice outlines which personal data are collected in the core services. It also provides a detailed explanation of the types of data collected and how these data are processed, with further details available in the Google Cloud Privacy Notice.

Google categorizes personal data into "Customer personal data" and "Service data." Customer personal data includes personal data uploaded to Google Workspace for Education, stored, sent, or received via the core services by the student or the school, such as students’ usernames, passwords, addresses, phone numbers, and profile pictures. These are data provided directly by the customer (school owner) to Google. Service data refers to data collected by Google during students’ use of the core services. Examples include account information, student activity, communication and interaction details, service usage data, location data, settings, apps, browsers, and devices used. It also includes billing information required for licensing Google Workspace for Education and information provided by users in support tickets. Although billing information and support ticket data are provided by the school owner as Google's customer, these are classified as Service data, not Customer personal data.

The Google Cloud Privacy Notice explains what personal data are collected as service data, who they are shared with, and the purposes of the collection. Google generally does not share service data with third parties but may share it in specific cases, such as with subcontractors, school administrators (with consent from the student or parent), or when using third-party services such as Google Marketplace. The data may also be used for external processing by Google’s partners or other third parties, as directed by Google and in compliance with Google’s privacy policy.

The purpose of collecting service data includes offering Cloud services, providing recommendations for more efficient Cloud usage, improving and offering other services from Google or third parties, providing technical support, protecting users and Google from security breaches and fraud, and fulfilling legal obligations. Under this agreement, Google is the controller for service data, while the customer is the controller for customer data according to the Google Cloud Processing Amendment.

If the customer (school owner) wishes to be the controller for both service data and customer data, they can sign the Google Workspace for Education Service Data Addendum, which activates the Supplemental Google Cloud Privacy Notice. The terms in the Google Cloud Privacy Notice still apply, except where they differ in the Supplemental Google Cloud Privacy Notice. The school owner becomes the controller for service data for the purpose of providing the service, while Google retains its role as a controller for certain uses of personal data as described in the Supplemental Google Cloud Privacy Notice.

This division of responsibilities ensures that the school owner can better align data processing with its obligations under privacy regulations.

# Appendix 4: Illustration of Recommendations

Figure 2 Illustration of recommendations when the school owner uses a managed ChromebookEt bilde som inneholder tekst, skjermbilde, diagram, Operativsystem

Automatisk generert beskrivelse

Figure 3 Illustration of recommendations when the school owner uses an unmanaged ChromebookEt bilde som inneholder tekst, skjermbilde, diagram, Operativsystem

Automatisk generert beskrivelse

Figure 4 Recommendation when the school owner uses a PC that is not a Chromebook

A screenshot of a computer

Description automatically generated



1. Service Data Addendum <https://support.google.com/a/answer/13865350?hl=en> [↑](#footnote-ref-2)
2. The use of DPM requires the Chrome browser to be used on a managed Chromebook. [↑](#footnote-ref-3)
3. A Chromebook is a type of PC produced by Google that uses the ChromeOS operating system. [↑](#footnote-ref-4)
4. ChromeOS Data Processor Mode Agreement, Points 2.1 to 2.6 under the heading “1 Data Processing Terms”,Point 13 regarding “Definitions”<https://www.google.com/chrome/dpchromeos/eu/index.html> [↑](#footnote-ref-5)
5. The use of DPM requires the Chrome browser to be used on a managed Chromebook. [↑](#footnote-ref-6)
6. A Chromebook is a type of computer produced by Google that runs the ChromeOS operating system. [↑](#footnote-ref-7)
7. The background for this recommendation is that Google acts as the controller for all personal data processed in the additional services. The national DPIA project has evaluated the additional services YouTube and Google Search and Assistant. However, as Google is the controller for other additional services as well, this recommendation applies to all additional services, including those not explicitly assessed by the national DPIA project. <https://support.google.com/a/answer/181865#zippy=%2Cturn-services-on-or-off-for-users%2Cadditional-services-with-an-individual-on-or-off-control> [↑](#footnote-ref-8)
8. Using Data Processor Mode (DPM) requires that the Chrome browser is used on a managed Chromebook. [↑](#footnote-ref-9)
9. The background for this recommendation is that Google acts as the controller for the processing of personal data (both *customer data* and *service data*) occurring in "Optional Services". See Point 1.8 "Optional Services" in the [ChromeOS Data Processor Mode Agreement](https://www.google.com/chrome/dpchromeos/eu/index.html). [↑](#footnote-ref-10)
10. <https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/nasjonal-dpia-for-google/bruk-av-tilleggstjenestene-i-google-workspace-for-education/> [↑](#footnote-ref-11)
11. <https://workspace.google.com/intl/en/terms/user_features/> [↑](#footnote-ref-12)
12. For example, YouTube, Gmail, Chrome browser, Google Maps, Google Translate, and Google Calendar. [↑](#footnote-ref-13)
13. SaaS, or Software as a Service, is a model where software is delivered over the internet. Users access applications via web browsers without needing local installation. The services are hosted in the cloud and often offered on a subscription basis. [↑](#footnote-ref-14)
14. Google Workspace for Education Privacy Notice, Intruduction

    (<https://workspace.google.com/terms/education_privacy/#privacy-police-revamp-intro>) [↑](#footnote-ref-15)
15. Service summary for Google Workspace Services (Core services and Other services) (<https://workspace.google.com/terms/user_features/>) [↑](#footnote-ref-16)
16. <https://support.google.com/a/answer/182442?hl=en> [↑](#footnote-ref-17)
17. Specifically,"customer personal data." Google is the controller for personal data that is also classified as "service data" and processed in the core services of Google Workspace for Education. [↑](#footnote-ref-18)
18. More precisely, the municipality is the controller for "customer data" in Google Workspace for Education, and Google acts as the processor for "customer data." For further details, see below under "Google’s processing of personal data." [↑](#footnote-ref-19)
19. <https://workspace.google.com/intl/en/terms/user_features/> [↑](#footnote-ref-20)
20. Google introduced Data Processor Mode for the Chrome browser on managed Chromebooks (ChromeOS) in Norway in spring 2024. By enabling Data Processor Mode for Chrome products, the school owner becomes the sole controller, and Google acts as the processor. This functionality must be activated. For further details, see below under "Google’s processing of personal data." [↑](#footnote-ref-21)
21. The municipality is the school owner for public schools at the primary level, the county municipality for secondary schools, and the top management for private schools. [↑](#footnote-ref-22)
22. The General Data Protection Regulation (GDPR) is incorporated into Norwegian law through the Personal Data Act. [↑](#footnote-ref-23)
23. For guidance on this selection of the primary legal basis for Norwegian school owners, see the project's guidance published on KS.no: <https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/behandlingsgrunnlag-for-google-workspace-for-education/> [↑](#footnote-ref-24)
24. For proposals regarding the various supplementary legal bases, see the project's suggested record of processing activities published on KS.no: <https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/forslag-til-behandlingsprotokoll-for-kjernetjenestene-i-google-workspace-for-education/> [↑](#footnote-ref-25)
25. <https://workspace.google.com/intl/no/terms/education_privacy/> [↑](#footnote-ref-26)
26. <https://workspace.google.com/intl/no/terms/education_privacy/> [↑](#footnote-ref-27)
27. Core services, supplemental services, or other products like the Chrome browser or the ChromeOS operating system. [↑](#footnote-ref-28)
28. ChromeOS on a Chromebook or other operating systems such as Windows on a PC. [↑](#footnote-ref-29)
29. <https://workspace.google.com/terms/education_privacy/#privacy-police-revamp-your-info> [↑](#footnote-ref-30)
30. <https://workspace.google.com/terms/education_privacy/#privacy-police-revamp-your-info> og <https://cloud.google.com/terms/cloud-privacy-notice-supplement> [↑](#footnote-ref-31)
31. <https://www.google.com/chrome/dpchromeos/eu/index.html> [↑](#footnote-ref-32)
32. Verified in a meeting with Google on March 11, 2024, and in an email sent on the same date. [↑](#footnote-ref-33)
33. The complete list can be found in a dedicated tab within the record of processing activities (see the proposed record of processing). This is an overview of all personal data in the solution, not tied to individual purposes, and is not linked to whether the data is processed by a controller or a processor. [↑](#footnote-ref-34)
34. "Personal data regarding racial or ethnic origin, political opinions, religion, philosophical beliefs, or trade union membership," "genetic and biometric data," and "health data or information concerning an individual's sexual relationships or sexual orientation." [↑](#footnote-ref-35)
35. See Table 1 Overview over who is a controller and who is a processor. [↑](#footnote-ref-36)
36. <https://workspace.google.com/intl/no/terms/education_privacy/> [↑](#footnote-ref-37)
37. <https://cloud.google.com/terms/cloud-privacy-notice> [↑](#footnote-ref-38)
38. Service data is similarly defined in the Chrome services (<https://support.google.com/chrome/a/answer/14316192?hl=en-IN&visit_id=638699548975939322-390431313&rd=1>) [↑](#footnote-ref-39)
39. See the purpose descriptions in the Google Cloud Privacy Notice (<https://cloud.google.com/terms/cloud-privacy-notice>). [↑](#footnote-ref-40)
40. By "the solution," we refer to the core services and AppSheet in Google Workspace for Education, ChromeOS, and the Chrome browser with Data Processor Mode enabled on a managed Chromebook. [↑](#footnote-ref-41)
41. See the suggested record of processing activities for Google Workspace for Education: <https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/forslag-til-behandlingsprotokoll-for-kjernetjenestene-i-google-workspace-for-education?trk=public_post_comment-text> [↑](#footnote-ref-42)
42. The Criminal Procedure Act, Chapter 15. <https://lovdata.no/lov/1981-05-22-25> [↑](#footnote-ref-43)
43. The Auditor General Act, § 12. <https://lovdata.no/lov/2004-05-07-21> [↑](#footnote-ref-44)
44. GDPR Article 5(1)(a). [↑](#footnote-ref-45)
45. [The Ministry of Education and Research, in a letter dated June 19, 2024, addressed to KS, has confirmed that this is the appropriate legal basis for processing.](https://www.ks.no/contentassets/c3c0b09667ad41e3a0eee2f6bdebe9e9/Svar-pa-henvendelse-om-behandlingsgrunnlag-for-bruk-av-digitale-leringsplattformer.pdf). [↑](#footnote-ref-46)
46. Education Act §§ 1-1 and 11-1. <https://lovdata.no/dokument/NL/lov/2023-06-09-30?q=oppl%C3%A6ringsloven> [↑](#footnote-ref-47)
47. As noted by the Danish Data Protection Agency in the Chromebook case on July 10, 2024 (Ref. No. 2023-431-0001). [↑](#footnote-ref-48)
48. See an example from Bergen Municipality on how school owners can inform about the use of Google Workspace for Education in schools: <http://193.161.171.199/innbyggerhjelpen/barnehage-og-skole/grunnskole/grunnskoleopplaring/googleverktoy-i-bergensskolen> [↑](#footnote-ref-49)
49. Cf. Juridika.no legal commentary on GDPR Article 5. [↑](#footnote-ref-50)
50. GDPR Article 5(1)(b). [↑](#footnote-ref-51)
51. GDPR Article 5(1)(b). [↑](#footnote-ref-52)
52. The Education Act § 1-1. <https://lovdata.no/dokument/NL/lov/2023-06-09-30?q=oppl%C3%A6ringsloven> [↑](#footnote-ref-53)
53. Framework for Basic Skills, [2.1 Digital skills as a basic skill](https://www.udir.no/laring-og-trivsel/rammeverk/rammeverk-for-grunnleggende-ferdigheter/2.1-digitale-ferdigheter/) [↑](#footnote-ref-54)
54. The Education Act § 28-1. <https://lovdata.no/dokument/NL/lov/2023-06-09-30?q=oppl%C3%A6ringsloven> [↑](#footnote-ref-55)
55. GDPR Article 6(4). [↑](#footnote-ref-56)
56. See Appendix 2: Assessment of whether Google's processing of personal data for its own purposes in the core services is compatible with the school owner's original purpose under the Education Act. [↑](#footnote-ref-57)
57. GDPR Article 5(1)(b). [↑](#footnote-ref-58)
58. GDPR Article 5(1)(c). [↑](#footnote-ref-59)
59. Juridka,no legal commentary on GDPR Article 5. [↑](#footnote-ref-60)
60. GDPR Article 5(1)(d). [↑](#footnote-ref-61)
61. GDPR Article 5(1)(e). [↑](#footnote-ref-62)
62. Google additionally takes up to 180 days before data is guaranteed to be deleted from all systems. [↑](#footnote-ref-63)
63. GDPR Article 5(1)(f). [↑](#footnote-ref-64)
64. GDPR Articles 13–14. [↑](#footnote-ref-65)
65. See examples from Bergen Municipality (<https://www.bergen.kommune.no/innbyggerhjelpen/barnehage-og-skole/grunnskole/grunnskoleopplaring/googleverktoy-i-bergensskolen>), Stavanger Municipality (<https://www.stavanger.kommune.no/barnehage-og-skole/skole/ikt-i-stavangerskolen/personvern-i-stavangerskolen/>) and Lillesand Municipality (<https://sites.google.com/lillesandskolen.no/lillesandskolen-digital/hjem>) for suggestions on how this can be implemented. [↑](#footnote-ref-66)
66. GDPR Article 15. [↑](#footnote-ref-67)
67. <https://services.google.com/fh/files/misc/gsuite_dsr_customer_guide.pdf> [↑](#footnote-ref-68)
68. <https://support.google.com/a/answer/6396995?hl=en> [↑](#footnote-ref-69)
69. GDPR Article 16. [↑](#footnote-ref-70)
70. GDPR Article 17. [↑](#footnote-ref-71)
71. GDPR Article 21. [↑](#footnote-ref-72)
72. GDPR Article 18. [↑](#footnote-ref-73)
73. GDPR Article 20. [↑](#footnote-ref-74)
74. GDPR Article 22. [↑](#footnote-ref-75)
75. <https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/innhenting-av-den-registrertes-mening/> [↑](#footnote-ref-76)
76. The municipality is the school owner for public schools at the primary level, the county municipality for secondary schools, and the top management for private schools. [↑](#footnote-ref-77)
77. The General Data Protection Regulation (GDPR) is incorporated into Norwegian law through the Personal Data Act. [↑](#footnote-ref-78)
78. More precisely, Google is the controller for "Service data," which includes more than just "metadata." For a more detailed description of what constitutes service data, see the main document of the DPIA under the heading "Service data." In this memo, however, we use the term "metadata," as it is Google's processing of students' activity data that presents challenges for Norwegian school owners' obligations under the Education Act. [↑](#footnote-ref-79)
79. The purposes are outlined in the Google Workspace for Education Privacy Notice: <https://workspace.google.com/intl/no/terms/education_privacy/#privacy-police-revamp-your-info> [↑](#footnote-ref-80)
80. Letter from the Ministry of Education to KS dated September 20, 2024. [↑](#footnote-ref-81)
81. For our assessment, see Appendix 2. [↑](#footnote-ref-82)
82. Users under 18 years of age who use Google Workspace for Education. [↑](#footnote-ref-83)
83. Letter addressed to KS from the Ministry of Education dated July 19, 2024: <https://www.ks.no/contentassets/c3c0b09667ad41e3a0eee2f6bdebe9e9/Svar-pa-henvendelse-om-behandlingsgrunnlag-for-bruk-av-digitale-leringsplattformer.pdf> [↑](#footnote-ref-84)
84. “Service data is used to deliver and maintain the services that schools and students use, as well as to improve the security and reliability of these services.”, cf. Google Workspace for Education Privacy Notice [↑](#footnote-ref-85)
85. ChromeOS Data Processor Mode Agreement, Section 13 "Definitions," "Legitimate Business Purposes (ii)." <https://www.google.com/chrome/dpchromeos/eu/no/index.html> [↑](#footnote-ref-86)
86. <https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/formalsbegrensning/> [↑](#footnote-ref-87)
87. Personal data about how users utilize Google Workspace for Education: Google processes personal data regarding how users engage with the solution. This is largely classified as "metadata." Metadata, often referred to as diagnostic data, includes information about software errors, operational status, performance data, and data from devices using GWFE, such as device identifiers and IP addresses. These data points are indirectly identifiable personal data, meaning they qualify as personal data because Google can potentially identify individuals. However, Google's purpose for processing this data is not to identify individual students, teachers, or municipal employees using Google Workspace for Education. Instead, the purpose is to enhance security and availability of the solution, cf. <https://cloud.google.com/terms/cloud-privacy-notice> [↑](#footnote-ref-88)
88. <https://workspaceupdates.googleblog.com/2023/06/improvements-for-client-side-encryption.html> [↑](#footnote-ref-89)