common sense®
Privacy Program

Standard Privacy Report for Microsoft Office 365 Education

✓ 88% Pass

Last updated August 12, 2021

Overview

Microsoft Office 365 Education is a collection of online services that allows students to collaborate and share their schoolwork. Students and educators are eligible for Office 365 Education for free, which includes Outlook, Word, Excel, PowerPoint, OneNote, Publisher, and Access. In addition, Office 365 Education includes classroom tools such as Exchange, OneDrive, SharePoint, Skype for Business, Teams, Sway, Forms, Stream, Flow, PowerApps, School Data Sync, and Bookings.

Microsoft's terms state children can access communication services, like Outlook and Skype, and can freely communicate and share data with other users of all ages. When users are signed in, some products may display a user's name or username and their profile photo as part of their use of Microsoft products, including in a user's communications, social interactions, and public posts. Microsoft's terms state they provide a privacy dashboard that allows users to control some of the data Microsoft processes through their use of a Microsoft account on the Microsoft privacy dashboard. From here, the terms state users can view and clear their browsing, search, and location data associated with their Microsoft account. Microsoft's terms state they are committed to protecting the security of its users' personal data. Microsoft uses a variety of security technologies and procedures to help protect users' personal data from unauthorized access, use, or disclosure. If a user uses a Microsoft product provided by an school or district they are affiliated with, or use an email address provided by a school or district to access Microsoft products, Microsoft may share certain data, such as interaction data and diagnostic data to enable a school or district to manage the products.

Microsoft Office 365 Education can be accessed through its website, and is available for download at their iOS App Store Homepage, and their Google Play Store Homepage. The Privacy Statement and Terms of Use used for this evaluation can be found on Microsoft Office 365 Education's website. This evaluation is intended to provide key information about Microsoft Office 365 collection and use of data for for Education users. Where there are terms that differ, as with the limitations on advertising in Office 365 for Education take precedence, followed by Microsoft's Privacy Statement.

Additionally, other relevant policies used for this evaluation include:

- Privacy Principles
- Microsoft Services Agreement
- Data Collection Summary

Safety

Microsoft's terms state children can access communication services, like Outlook and Skype, and can freely communicate and share data with other users of all ages. When users are signed in, some products may display a user's name or username and their profile photo as part of their use of Microsoft products, including in a user's communications, social interactions, and public posts. The terms state that when a user creates a personal Microsoft account, they will be asked to provide certain personal data and they will assign a unique ID number to identify a user's account and associated information. While some products, such as those involving payment, require a real name, the terms state users can sign in and use other Microsoft products without providing their real name. Some data a user provides, such as their display name, email address, and phone number, can be used to help others find and connect with that user within Microsoft products.

In addition, the terms state that users should be aware that when they share their content with other people, it may become publicly visible to others. Microsoft's terms state they also provide parental tools called Family Features, which allow parents and kids to build trust based on a shared understanding of what behaviors, websites, apps, games, physical locations, and spending is right in their family. Parents can create a family account by going to https://account.microsoft.com/family and inviting their kids or other parents to join.

Privacy

Microsoft's terms state they provide a privacy dashboard that allows users to control some of the data Microsoft processes through their use of a Microsoft account on the Microsoft privacy dashboard. From here, the terms state users can view and clear their browsing, search, and location data associated with their Microsoft account. The terms state many of Microsoft's products require some personal data to provide users with its services. The data Microsoft services can collect include: first and last name, email address, postal address, phone number, password credentials, and data about users such as their age, gender, country, and preferred language.

In addition, the terms state Microsoft also obtains data about users from third parties, such as data brokers from which Microsoft purchases demographic data to supplement the data they collect, and from services that make user-generated content from their service available to others, such as local business reviews or public social media posts. In carrying out these purposes, the terms state Microsoft combines data they collect from different contexts (for example, from a user's use of two Microsoft products) or obtain from third parties to give users a more seamless, consistent, and personalized experience, to make informed business decisions, and for other legitimate purposes.

The terms say a user's data is not sold to third parties, and the terms say that personal information will be used or otherwise processed only to provide users the services including purposes compatible with providing those services. Also, Microsoft's Online Service Terms state they will not use or otherwise process personal information or derive information from it for any advertising or similar commercial purposes. However, parents and teachers should be aware that the Microsoft's privacy policy states they may use personal information for marketing and advertising purposes for other Microsoft products.

Security

Microsoft's terms state they are committed to protecting the security of its users' personal data. Microsoft uses a variety of security technologies and procedures to help protect users' personal data from unauthorized access, use, or disclosure. For example, the terms state Microsoft stores the personal data users provide on computer systems that have limited access and are in controlled facilities and protect the data users entrust to Microsoft through strong security and encryption. In addition, the terms state security is central to compliance with FERPA, which requires the protection of student information from unauthorized disclosures. The terms state educational institutions that use cloud computing should have contractual reassurances from a technology vendor like Microsoft that they will manage sensitive student data appropriately.

In addition, the terms state Microsoft uses data to protect the safety of their products and their customers. Microsoft's security features and products can disrupt the operation of malicious software and notify users if malicious software is found on their devices. The terms also state Microsoft uses data they collect to develop product updates and security patches. For example, the terms state Microsoft may use information about a user's device’s capabilities, such as available memory, to provide users with a software update or security patch. The terms also state updates and patches are intended to maximize users' experience with Microsoft's products, help users' protect the privacy and security of their data, provide new features, and ensure a user's device is ready to process updates. Lastly, the terms state Microsoft complies with data protection laws, including providing security breach notification to users.

Compliance

If a user uses a Microsoft product provided by an school or district they are affiliated with, or use an email address provided by a school or district to access Microsoft products, Microsoft may share certain data, such as interaction data and diagnostic data to enable a school or district to manage the products. The data associated with a school account, and how it will be used, is generally similar to the use and collection of data associated with a personal Microsoft account. If a school uses Azure Active Directory (AAD) to manage the account it provides to users, then a user can use their school account to sign in to Microsoft products, such as Office 365, and third-party products. If required by a school or district, users may also be asked to provide a phone number or an alternative email address for additional security verification.

In its terms, Microsoft agrees to obtain parental consent before collecting or disclosing personal information from minors. In addition, Microsoft states it may be designated as a "school official" with "legitimate educational interests" in student data as defined under FERPA. Microsoft also commits to using student data only to provide schools and districts with its cloud services and compatible purposes (such as improving malware detection), and does not mine student data for advertising. Lastly, the terms state Microsoft contractually commits not to disclose student data except as the educational institution directs, or as described in a school or district contract. Furthermore, the terms state schools that provide education records to Microsoft through their use of a Microsoft cloud service can be assured that those records are subject to stringent contractual restrictions regarding their use and disclosure.

Overall Score

Every privacy rating includes an overall score. A higher score (up to 100%) means the product provides more transparent privacy policies with better practices to protect user data. The score is best used is as an indicator of how much additional work a person will need to do to make an informed decision about a product.

	Basic Score	Full Score
Comprehensive Assessment	88	72

Concerns

The privacy evaluation process summarizes the policies of an application or service into concern categories based on a subset of evaluation questions that can be used to quickly identify particular practices of a vendor's policies. These concerns are composed of evaluation questions that can be used to calculate scores relative to that concern.

Concern	Basic Score	Full Score
Data Collection: Protecting personal information	75	60
Data Sharing: Protecting data from third parties	100	95
Data Security: Protecting against unauthorized access	100	95

Concern	Basic Score	Full Score
Data Rights: Controlling rights to data	88	95
Data Sold: Preventing sale of data	75	55
Data Safety: Promoting responsible use	50	45
Ads & Tracking: Prohibiting the exploitation of users' decision making process	92	85
Parental Consent: Protecting children’s personal information	100	75
School Purpose: Following student data privacy laws	100	45

Statutes

Each statute or regulation is associated with one or more evaluation questions. As such, we can calculate scores for each statute or regulation using only those questions associated with the statute or regulation. Each specific statute or regulation's score serves as an indirect proxy indicating the likelihood of the application or service satisfying all of its compliance obligations.

Statute	Basic Score	Full Score
California Online Privacy Protection Act (CalOPPA)	92	81
Children's Online Privacy Protection Act (COPPA)	85	74
Family Educational Rights and Privacy Act (FERPA)	94	68
Student Online Personal Information Protection Act (SOPIPA)	96	74
General Data Protection Regulation (GDPR)	96	82

Privacy Policy Details

1: Transparency

1.1: POLICY VERSION

- Privacy policies do indicate a version or effective date.
- Privacy policies indicate a changelog or past policy version is available.

1.2: POLICY NOTICE

✓ Users are notified if there are any material changes to the policies.

- Privacy policies indicate the method used to notify a user when policies are updated.

1.3: POLICY CHANGES

✓ Users are notified prior to any material changes to the policies.

⚠ Changes to the policies are effective immediately and continued use of the product indicates consent.

1.4: POLICY COVERAGE

- Privacy policies indicate the products that are covered by the policies.

1.5: POLICY CONTACT

✓ Users can contact the vendor about any privacy policy questions, complaints, or material changes to the policies.

1.6: POLICY PRINCIPLES

- Privacy policies do indicate any privacy principles, layered notices, or a table of contents.

1.7: POLICY LANGUAGE

- Privacy policies are available in multiple languages.

1.8: INTENDED USE

- Intended for children under 13.

⚠ Unclear whether intended for teens.

- Intended for adults over 18.

⚠ Unclear whether intended for parents or guardians.

- Intended for students.

⚠ Unclear whether intended for teachers.

2: Focused Collection

2.1: DATA COLLECTION

⚠ Personally identifiable information (PII) is collected.

- The categories of collected personally identifiable information are indicated.

⚠ Geolocation data are collected.

⚠ Unclear whether this product collects biometric or health data.

- ⚠ Behavioral data are collected.
- ⚠ Sensitive data are collected.
- ⚠ Non-personally identifiable information is collected.
- ⚠ Unclear whether free or reduced lunch status is collected.

2.2: DATA SOURCE

- ⚠ Personal information or education records are collected from preK-12 students.
- ⚠ Personal information from children under 13 years of age is collected online.

2.3: DATA EXCLUSION

- ⚠ Unclear whether specific types of personal information are not collected.
- ⚠ Unclear whether specific types of collected information are excluded from the privacy policy.

2.4: DATA LIMITATION

- ✓ Collection or use of data is limited to product requirements.

3: Data Sharing

3.1: DATA SHARED WITH THIRD PARTIES

- Collected information is shared with third parties.
- The categories of information shared with third parties are indicated.

3.2: DATA USE BY THIRD PARTIES

- The purpose for sharing a user's personal information with third parties is indicated.
- ⚠ Data are shared for analytics.
- ✓ Data are not shared for research and/or product improvement.
- ✓ Data are not shared for third-party advertising and/or marketing.

3.3: DATA NOT SHARED WITH THIRD PARTIES

- Unclear whether there are specific categories of information that are not shared with third parties.

3.4: DATA SOLD TO THIRD PARTIES

- ✓ Data are not sold or rented to third parties.

3.5: THIRD-PARTY DATA ACQUISITION

⚠ Personal information from users is acquired from third parties.

3.6: THIRD-PARTY LINKS

⚠ Links to third-party external websites are not age-appropriate.

3.7: THIRD-PARTY DATA ACCESS

⚠ Third parties are authorized to access a user's information.

3.8: THIRD-PARTY DATA COLLECTION

⚠ Personal information of users is collected by a third party.

3.9: THIRD-PARTY DATA MISUSE

⚠ Unclear whether personal information can be deleted from a third party if found to be misused.

3.10: THIRD-PARTY SERVICE PROVIDERS

- Data are shared with third-party service providers.
- The roles of third-party service providers are indicated.

3.11: THIRD-PARTY AFFILIATES

- The categories of third parties that receive personal information are indicated.

3.12: THIRD-PARTY POLICIES

- Links to privacy policies of third-party companies are not available.

3.13: THIRD-PARTY DATA COMBINATION

⚠ Data can be combined with data from third-party sources.

⚠ Unclear whether data shared with third parties can be combined by third parties for their own purposes.

3.14: THIRD-PARTY AUTHENTICATION

- Social or federated login is supported.

⚠ Personal information from social or federated login providers is collected.

⚠ Personal Information is shared with social or federated login providers.

3.15: DE-IDENTIFIED OR ANONYMIZED DATA

- User information is shared in an anonymous or deidentified format.

⚠ Unclear whether the vendor describes their deidentification process of user information.

3.16: THIRD-PARTY CONTRACTUAL OBLIGATIONS

✓ Contractual limits are placed on third-party data use.

✓ Contractual limits prohibit third parties from reidentifying deidentified information.

4: Respect for Context

4.1: DATA USE

✓ Use of information is limited to the purpose for which it was collected.

- The purpose for which data atr collected is indicated.

4.2: DATA COMBINATION

✓ Combined information is treated as personally identifiable information (PII).

4.3: DATA NOTICE

✓ Notice is provided if the context in which data are collected changes.

4.4: DATA CHANGES

✓ Consent is obtained if the practices in which data are collected change.

4.5: POLICY ENFORCEMENT

✓ Accounts may be terminated if users engage in any prohibited activities.

5: Individual Control

5.1: USER CONTENT

⚠ Users can create or upload content.

5.2: USER CONSENT

✓ Opt-in consent is requested from users at the time personal information is collected.

5.3: REMEDY PROCESS

✓ A grievance or remedy mechanism is available for users to file a complaint.

5.4: DATA SETTINGS

✓ Users can control their information through privacy settings.

5.5: DATA DISCLOSURE

✓ Users can opt out from the disclosure or sale of their data to a third party.

⚠ Unclear whether users can request to know what personal information has been shared with third parties for commercial purposes.

✓ Notice is provided in the event the vendor receives a government or legal request for a user’s information.

5.6: INTELLECTUAL PROPERTY

✓ Users retain ownership of their data.

✓ A copyright license is claimed to data or content collected from a user.

⚠ Unclear whether any copyright license to a user's data is limited in scope or duration.

✓ Notice is provided to users when their content is removed or disabled because of an alleged copyright violation.

6: Access and Accuracy

6.1: DATA ACCESS

✓ Processes to access and review user data are available.

✓ Permissions, roles, or access controls are available to restrict who has access to data.

✓ Processes to review data are available for the school, parents, or students.

6.2: DATA INTEGRITY

✓ The vendor does maintain the accuracy of data they collect.

6.3: DATA CORRECTION

✓ Processes to modify inaccurate data are available.

✓ Processes for the school, parents, or students to modify data are available.

● The time period for the vendor to modify inaccurate data is indicated.

6.4: DATA RETENTION

● A data-retention policy is available.

✓ The retention time period of a user's data can be changed upon a valid inspection request.

6.5: DATA DELETION

✓ Data are deleted when no longer necessary.

✓ A user's data are deleted upon account cancellation or termination.

✓ Processes to delete user data are available.

✓ Processes for the school, parents, or students to delete data are available.

● The time period for the vendor to delete data is indicated.

6.6: DATA PORTABILITY

✓ Processes to download user data are available.

✓ A user can assign an authorized account manager or legacy contact.

7: Data Transfer

7.1: DATA HANDLING

⚠ User information can be transferred to a third party.

⚠ Notice is provided to users if the vendor assigns its rights or delegates its duties to another company.

⚠ Unclear whether users are notified if their information is transferred to a third party.

7.2: TRANSFER REQUEST

⚠ Unclear whether user information can be deleted prior to its transfer to a third party.

7.3: ONWARD CONTRACTUAL OBLIGATIONS

⚠ Unclear whether third-party transfers are contractually required to use the same privacy practices.

8: Security

8.1: USER IDENTITY

⚠ A user's identity is verified with additional personal information.

8.2: USER ACCOUNT

● Account creation is required.

● Parental controls or managed accounts are available.

✓ Two-factor account protection is available.

8.3: THIRD-PARTY SECURITY

- ✓ Third-party contractual security protections are required.

8.4: DATA CONFIDENTIALITY

- ✓ Industry best practices are used to protect data.
- ✓ Employee or physical access to user information is limited.

8.5: DATA TRANSMISSION

- ✓ All data in transit are encrypted.

8.6: DATA STORAGE

- ✓ All data at rest are encrypted.
- ✓ Personal information of users is not stored with a third party.

8.7: DATA BREACH

- ✓ Notice is provided in the event of a data breach.

8.8: DATA OVERSIGHT

- ✓ Data-privacy and security-compliance audits are performed.

9: Responsible Use

9.1: SOCIAL INTERACTIONS

- Users can interact with trusted users and/or students.
- ⚠ Users can interact with untrusted users, including strangers and/or adults.
- ⚠ Profile information is shared for social interactions.

9.2: DATA VISIBILITY

- ⚠ Personal information is displayed publicly.
- ✓ Users can control how their data are displayed.

9.3: MONITOR AND REVIEW

- ⚠ User-created content is not reviewed, screened, or monitored by the vendor.
- ⚠ User-created content is not filtered for personal information before being made publicly visible.
- ⚠ Unclear whether social interactions between users are moderated.
- ⚠ Unclear whether social interactions of users are logged.

9.4: REPORT CONTENT

⚠ Unclear whether users can filter or block inappropriate content.

⚠ Unclear whether users can report abuse or cyberbullying.

9.5: INTERNET SAFETY

⚠ Unclear whether the vendor provides links to tools or processes that support safe and appropriate social interactions.

10: Advertising

10.1: VENDOR COMMUNICATIONS

✓ A user can receive service- or administrative-related communications from the vendor.

10.2: TRADITIONAL ADVERTISING

⚠ Traditional or contextual advertisements are displayed.

10.3: BEHAVIORAL ADVERTISING

✓ Behavioral or targeted advertising is not displayed.

10.4: AD TRACKING

✓ Data are not collected by third-party advertising or tracking services.

✓ Data are not used to track and target advertisements on other third-party websites or services.

✓ Data profiles are not created and used for data enhancement, and/or targeted advertisements.

10.5: FILTERED ADVERTISING

✓ Children do not receive any inappropriate advertisements.

10.6: MARKETING COMMUNICATIONS

⚠ The vendor can send marketing messages.

⚠ The vendor does provide promotional sweepstakes, contests, or surveys.

10.7: UNSUBSCRIBE

✓ Users can opt out of traditional, contextual, or behavioral advertising.

✓ Users can opt out or unsubscribe from marketing communications.

10.8: DO NOT TRACK

⚠ Vendor does not respond to Do Not Track or other opt-out mechanisms.

- The vendor does provide a method for users to opt-out from third-party tracking.

11: Compliance

11.1: CHILDREN UNDER 13

- Vendor does have actual knowledge that personal information from users under 13 years of age is collected.

✓ Children's privacy is applicable.

✓ Account creation is restricted for users under 13 years of age.

✓ Vendor does restrict in-app purchases for users under 13 years of age.

⚠ Unclear whether the vendor participates in an FTC-approved COPPA safe harbor program.

11.2: STUDENTS IN K–12

- Product is primarily used by, designed for, and marketed toward students in grades preK–12.
- Product does create education records.

✓ Notification of a contract or additional rights is provided.

⚠ Unclear whether this product designates the vendor as a school official.

11.3: PARENTAL CONSENT

✓ Parental consent is required.

⚠ Unclear whether this product limits parental consent with respect to third parties.

✓ Parents can withdraw consent for the further collection of their child's information.

✓ Children's personal information is deleted if collected without parental consent.

✓ Parental consent notice and method for submission are provided.

⚠ Unclear whether the vendor can use collected information to support the "internal operations" of the product.

⚠ Unclear whether this product indicates COPPA parental consent exceptions.

⚠ Unclear whether the vendor indicates FERPA parental consent exceptions.

⚠ Unclear whether this product discloses directory information.

⚠ Unclear whether this product transfers parental consent obligations to the school or district.

11.4: LEGAL REQUIREMENTS

- The legal jurisdiction that applies to the laws governing any dispute is indicated.

⚠ A user is required to waive the right to a jury trial, or settle any disputes by arbitration.

⚠ A user is required to waive the right to join a class action lawsuit.

⚠ A vendor will disclose personal information to law enforcement.

11.5: CERTIFICATION

⚠ Unclear whether the vendor has signed a privacy pledge or received a privacy certification.

11.6: INTERNATIONAL LAWS

- A user's data are subject to International data transfer or jurisdiction laws, such as the GDPR.

✓ The vendor has indicated it is a Data Controller or Data Processor.

Return to Privacy Evaluation

Common Sense Media provides this standard privacy report for use by the general public for research and education purposes only. The accuracy, completeness, or adequacy of the content provided or evaluation results derived from a product’s policies is not warranted or guaranteed.