Public Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR

https://www.dataprotection.ie/sites/default/files/uploads/2018-12/DPC_ChildrensRights_2019_English.pdf

Questions

1. What methods could organisations who collect and use children's personal data employ to easily convey this transparency information to children?
2. What approach should be used by organisations whose products or services are aimed at both adults and children? For example, should two separates sets of transparency information be provided that are each tailored according to the relevant audience?
3. At what age or in what circumstances should a child be able to make an access request to an organisation and receive a copy of their personal data? Is age the only relevant factor and if not, what other factors should be taken into consideration?
4. In what circumstances should a parent be able to make an access request and receive a copy of their child's personal data? Is there an upper age limit after which a parent should not be able to make an access request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an access request for the child's personal data?
5. How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy when organisations are dealing with access requests for the child's personal data?
6. At what age or in what circumstances should a child be able to make an erasure request to an organisation and have their personal data erased? Is age the only relevant factor and if not, what other factors should be taken into consideration?
7. In what circumstances should a parent be able to make an erasure request on behalf of their child and have their child's personal data erased? Is there an upper age limit after which a parent should not be able to make an erasure request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an erasure request?
8. If an online service provider is relying on consent as their legal basis (justification) for processing children's personal data, what methods could/should be used to verify that a child is 16 or over in order that the child is granted access to the online service without the need for parental consent?
9.
    a. What methods could/should online service providers use to ensure that the person providing consent in these circumstances is actually the holder of parental responsibility over the child?
    b. What constitutes a "reasonable effort" made by organisations to verify such consent is being given by a person who is actually the holder of parental responsibility over the child? How should "reasonable efforts" be measured in this regard?

10. Prior to 25 May 2018, there was no law setting the age of digital consent in Ireland, but many online service providers required users to be at least 13. If an online service provider now is aware that an existing user of their service is under 16, should the user be locked out of the service until they reach 16?
11. How should such online service providers ensure they comply with different ages of digital consent in different Member States?
12. In the case of marketing to a child, what factors should be taken into consideration when balancing an organisation's own legitimate interests in conducting direct marketing and the interests and rights of a child who is being marketed to?
13. Should organisations be prohibited from profiling children for marketing purposes? If so, should this be age-dependent or dependent on other factors? If so, what are these other factors?
14. What measures should organisations take to incorporate the principles of data protection by design and by default into the services and products that they offer to children?
15. Do you think products/services that are used by or offered to children should have built-in default privacy settings that vary according to the age and evolving capacities of a child? For example, should there be stricter privacy settings for younger children? How should these variations in the privacy settings be given effect?
16. Are there any other particular issues you would like to raise with the DPC in connection with the subject matter of this consultation?

Microsoft's Responses

1. What methods could organisations who collect and use children's personal data employ to easily convey this transparency information to children?

Organisations have an obligation under Article 12.1 of the GDPR to ensure that any transparency information about data processing which is addressed to a child should be in clear and plain language so that the child can understand it. There is no simple one-size-fits-all solution to achieve this. There are many different means companies can employ to achieve meaningful levels of transparency for children. Companies should adopt a creative approach to convey this information depending on the context of the processing and the types of data being processed.

It is important to remember that adults play a key role in helping younger children understand how their data is being processed, and we encourage adults to be involved and have oversight of children's online activities and promote responsible behaviour.

Microsoft has expressly stated its commitment to transparency as one of our core privacy principles, and we are deeply committed to being transparent about data collection and use so that users can make informed decisions. We also employ a combination of the methods set out as follows below with a view to meaningful transparency for children:

- We provide privacy information in a layered manner with a first layer of information offered via easy-to-read contextual notices, which provide information about privacy choices within the user interface. These contextual notices, sometimes called just-in-time notices, contain short, plain-language text to describe choices and visual cues to help users understand their options and to quickly move through their privacy choices during set-up.
- This first layer leads to our Microsoft Privacy Statement, which details Microsoft's data protection policies and practices in clear, straightforward language we believe a child could comfortably engage with.
- We also provide information about data collection, use, and controls in our consumer privacy Dashboard. See Appendix 1 for an example of how Microsoft makes use of this approach.
- As mentioned above, adults can play a critical role in helping younger children to understand and interact responsibly online. Indeed, we believe that a young child is increasingly likely to fully understand the

implications of their online experience if an adult can oversee the child's activities. To encourage this involvement, we provide further safeguards and controls for the adult to promote online safety and responsible behaviours for younger children. We enable a range of privacy-protective settings which are made available depending on the age and capabilities of children such as family account features, which enable families to stay connected and lets parents set stricter privacy settings for children's accounts. These settings can help increase visibility around children's online behavioural habits and give options to parents to implement activity reporting, screen time limits, location sharing, and content filters for their children. See Appendices 2 and 3 containing examples of family protections on our Xbox platform. These support the parents' critical role in helping educate children about data protection and safety online, which further contributes to transparency information for their children.

2. What approach should be used by organisations whose products or services are aimed at both adults and children? For example, should two separates sets of transparency information be provided that are each tailored according to the relevant audience?

Companies should strive to make the privacy information about their products and services intelligible to their diverse user base. This user base may include children, adults with varying levels of technical expertise and education, as well as individuals who may have cognitive and/or physical disabilities.

We don't believe creating two separate sets of transparency notices is necessary, or even the best way, to achieve the aims and objectives of transparency under the GDPR. We favour a clear, connected, and layered approach to deliver privacy information so that each user can understand and engage with the information at the level with which they are most comfortable.

People with different levels of technical expertise may want different levels of detail in their privacy documentation. For example, a busy parent may want to move through privacy settings quickly with contextual notices in a plain, easy-to-read format. A more technically sophisticated user may want to take a deep dive into data types and processing categories. Companies should endeavour to create a user experience whereby the user – regardless of age and demographic – can access the level of detail they desire. This may be achieved through clear, transparent notices complemented by family-friendly settings where parents can engage with the child as described above in the response to Question 1.

3. At what age or in what circumstances should a child be able to make an access request to an organisation and receive a copy of their personal data? Is age the only relevant factor and if not, what other factors should be taken into consideration?

The GDPR does not specify when, or in what circumstances, a child can make their own access request for their personal data. However, we believe that children of any age should have access to their personal data. Companies may facilitate this access through a range of tools, such as privacy dashboards which enable users to exercise control over their data.

Generally, we do not believe age should be the sole relevant factor. When designing systems to respond to data access requests, an organisation should be thoughtful about other relevant considerations and whether the

child understands the meaning of the right to access their data. Depending on the types of data being processed, the factors an organisation should remain cognisant of may include the following:

- the child's level of maturity and ability to make decisions;
- the nature of the personal data;
- any applicable court orders;
- any duty of confidence owed to the child;
- any consequences of allowing access to those with parental responsibility. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child if those with parental responsibility cannot access this information;
- any views the child has on whether their parents should have access to their personal data; and
- the needs or expectations of a parent in understanding their child's activities online.

To support scalable, global services, companies should consider these factors as part of a data protection by design strategy to establish a standard approach for responding to access requests from children.

4. In what circumstances should a parent be able to make an access request and receive a copy of their child's personal data? Is there an upper age limit after which a parent should not be able to make an access request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an access request for the child's personal data?

The GDPR does not specify when, or in what circumstances, a parent or guardian can make an access request for their child's personal data. However, a parent should be permitted to make an access request on behalf of the child if, on balance, it would be in the best interests of the child. This may occur where a child does not fully understand the right of access or how best to exercise the right in a privacy-protective manner.

To facilitate this parental access, companies can implement feature-sets and user experiences into their services which enable parents to make access requests for a child's data. For example, including the option of family-friendly settings in the user interface can be a sensible way to address this and help to promote online safety and responsible behaviour for children. As described above, Microsoft's Family Service contains parental controls and enables a parent to access their child's personal data when that child joins their family group within the Family Service. This provides an environment where a parent can have oversight of their child's online activities and which promotes an inclusive discussion about data protection and safety online.

In general, we think it is reasonable that the upper age limit for parents to be able to exercise rights of access to their child's personal data under GDPR should not exceed the statutory age of a "child" in their country unless the data subject has provided consent, which could be given through this type of family settings or similar feature.

We don't believe a joint request from the parent and child is the best way to afford more control over children's personal data. If a parent is authorised to act on their child's behalf, that authorisation should be relied upon for the parent to access the child's personal data.

5. How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy when organisations are dealing with access requests for the child's personal data?

If a child is competent and understands the rights in question, it should be generally appropriate for the child to exercise his or her access rights. Age is an important factor to determine whether a child has sufficient understanding of their rights and this should inform how companies strike the balance of access between the parent and the child. Other factors which could be taken into account are as described above in the above response to Question 3.

As we stated above in response to Question 4, at Microsoft we offer a Family Service through which we enable a parent to access their child's personal data if that child joins their family group within the Family Service. The purpose of the Family Service is so that parents can have oversight of their child's online activities and help ensure parents and children can discuss and make informed decisions about children's data protection and online safety. At the same time, the child has access to their personal data via our privacy Dashboard.

6. At what age or in what circumstances should a child be able to make an erasure request to an organisation and have their personal data erased? Is age the only relevant factor and if not, what other factors should be taken into consideration?

Under the GDPR, individuals have the right to have their personal data erased, without undue delay, by an organisation if certain grounds apply. As stated in the response to Question 5 above, if a child is competent and understands the rights in question, then we are of the view it is usually appropriate for the child to exercise his or her rights, and to make an erasure request or to authorise a parent to do so on the child's behalf. If the child is not competent, the holder of parental authority should exercise that right. Generally, age is not the sole relevant factor. It is important to weigh considerations such as children's online safety and behaviour and whether the child fully understands the permanent nature of this choice and the future implications of erasing their data.

Depending on the types of data being processed, when designing systems to respond to data erasure requests, an organisation should be thoughtful about other relevant considerations including the best interests of the child and the child's level of maturity and ability to make decisions. As noted above in the context of access requests, in order to support scalable, global services, companies should consider these factors as part of a data protection by design strategy to establish a standard approach for responding to erasure requests from children.

In general, we think it is reasonable that the upper age limit for parents being able to request erasure of their child's personal data should not exceed the statutory age of a "child" in their country unless the data subject has provided consent, which could be given through a feature like family settings.

7. In what circumstances should a parent be able to make an erasure request on behalf of their child and have their child's personal data erased? Is there an upper age limit after which a parent should not be able to make an erasure request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an erasure request?

In general, a parent should be permitted to make an erasure request if this is in the best interests of the child. This may occur where a child does not fully understand or appreciate the long-term impact of erasing their data. Companies may implement feature-sets and user experiences which enable parents to make erasure requests. Including the option of family-friendly settings into the user interface can be a sensible way to address this and help to promote online safety and good behaviour for children.

Microsoft's Family Service allows a parent to make an erasure request on behalf of their child if that child has joined the family within the Family Service. The purpose of Microsoft Family Service is so that parents can have oversight of their child's online activities and help ensure parents and children can discuss and make informed decisions about children's data protection and online safety. See Appendix 2 and Appendix 3 containing examples of such family protections on our Xbox platform.

In general, we think it is reasonable that the upper age limit should not exceed the statutory age of a "child" in their country unless the data subject has provided consent, which could be given through this type of family-friendly settings.

Generally, we don't believe a joint erasure request from the parent and child is the best way to afford more control over children's personal data. If a parent is authorised to act on their child's behalf, that authorisation should be relied upon for the parent to make an erasure request concerning the child's personal data.

8. If an online service provider is relying on consent as their legal basis (justification) for processing children's personal data, what methods could/should be used to verify that a child is 16 or over in order that the child is granted access to the online service without the need for parental consent?

When collecting personal data, an online service provider could implement an age gate to confirm a child is over the statutory age (16 years of age or over in Ireland). Microsoft utilises such an age gate on Microsoft account for this purpose that prompts users to enter their country and date of birth. Users who are younger than the statutory age of consent for their country will then be prompted for parental consent when they create their account or, in the case of existing users, when they sign in to their account. Whether a self-declaration of age should be sufficient depends on the types of services the service provider offers, balancing data minimisation principles with the risks of processing.

9. (a) What methods could/should online service providers use to ensure that the person providing consent in these circumstances is actually the holder of parental responsibility over the child?

   (b) What constitutes a "reasonable effort" made by organisations to verify such consent is being given by a person who is actually the holder of parental responsibility over the child? How should "reasonable efforts" be measured in this regard?

(a) It is very important that there are controls around the process of obtaining any parental consent and that the controller makes reasonable efforts to verify the consent is received from the holder of parental responsibility. Companies may implement different checks to achieve this. For example, companies may rely on the high standards afforded under the U.S. Children's Online Privacy Protection Act (COPPA) to verify parental consent for children's accounts across product platforms. Microsoft is guided by COPPA standards when verifying our parental consent and we believe our mechanisms will increasingly be informed by the guidance that develops around GDPR with regard to parental consent mechanisms.

(b) We believe COPPA sets out a strong benchmark for "reasonable efforts" to verify consent. Building on our COPPA processes, Microsoft prompts existing Microsoft account holders to provide their country and date of birth. Those account holders who are younger than the age of consent for their country will then be prompted for

parental consent when they sign into their account during a grace period. To verify their child's account, parents will authenticate to their Microsoft account; provide an electronic signature to give permission for their child to have a Microsoft account and authorise data collection and use as described in the Microsoft Privacy Statement; and receive confirmation that the account was created. Parents who cannot, or choose not, to go through this process can also contact Microsoft Customer Service and Support to verify age and identity based on appropriate government documents. After the grace period for existing users, the child's account will be blocked until the parent completes the consent and verification process. If a person creating a new Microsoft account is younger than the statutory age, they must obtain parental consent and verification before they can use the account.

We would welcome further clarification in this area. Until further guidance is issued as to what "reasonable efforts" means under the GDPR, companies should be permitted to rely on widely accepted frameworks (such as COPPA) to implement these parental consent requirements in the GDPR.

10. Prior to 25 May 2018, there was no law setting the age of digital consent in Ireland, but many online service providers required users to be at least 13. If an online service provider now is aware that an existing user of their service is under 16, should the user be locked out of the service until they reach 16?

This question implicates two competing concepts. Firstly, recognising that parental consent may be necessary to process the personal data of a child under the statutory age and secondly, understanding that a child enjoys individual rights to their personal data in accordance with the GDPR. In the scenario outlined in the question, a child may have up to three years of personal data built up in services which they have been using. It would seem disproportionate and contrary to the best interests of the child to lock them out of their service and deny them access to their personal data. At the same time, companies should strive to obtain parental consent where it is now required.

11. How should such online service providers ensure they comply with different ages of digital consent in different Member States?

As described above in the responses to Questions 8 and 9, online service providers could choose to implement an age gate and require parental consent before they collect personal data from children. To implement an age gate, services could ask for a date of birth and determine location and then, upon learning that a person is within the statutory definition of a "child" in their country, obtain parental consent or bar the child from using the service. This requires companies to adjust the age gate based on the laws in each Member State, which requires collecting information about where they child is located. As with date of birth, self-declaration of country should be sufficient, depending on the type of service.

12. In the case of marketing to a child, what factors should be taken into consideration when balancing an organisation's own legitimate interests in conducting direct marketing and the interests and rights of a child who is being marketed to?

If an organisation is planning on marketing to children specifically, then it is important to establish whether this marketing gives rise to a high risk to the rights and freedoms of the children. An organisation should process children's data in a manner that is fair and complies with all other data protection principles contained in the GDPR. Processing children's data requires a special degree of care and attention, and an organisation must have a lawful basis for its processing and should explain the processing in a transparent manner which is understandable by children.

At Microsoft, we understand the increased risks when processing children'. As stated in the Microsoft Privacy Statement, we do not deliver interest-based advertising to children identified as under 16 years of age in their Microsoft account.

13. Should organisations be prohibited from profiling children for marketing purposes? If so, should this be age-dependent or dependent on other factors? If so, what are these other factors?

It is important that appropriate safeguards are put in place when it comes to profiling children for marketing purposes. Factors such as the child's age, competence, and their ability to understand the marketing should be carefully considered when companies decide how to engage with children. Microsoft understands that family-friendly settings empowering parents to supervise and engage can be a very practical measure to promote responsible online activity for children.

As stated in our response to Question 12 above, Microsoft does not deliver interest-based advertising to children identified as under 16 years of age in their Microsoft account. We could understand if a prohibition against specific profiling of children for marketing purposes was to be put in place.

14. What measures should organisations take to incorporate the principles of data protection by design and by default into the services and products that they offer to children?

Companies can provide a combination of techniques to incorporate these principles. This might include providing feature settings across products and services which promote and protect children's privacy and communicating privacy information in a clear, straightforward, and transparent manner which can be understood by a child.

To help us achieve this principle, our Microsoft Privacy Statement details Microsoft's data protection policies and practices in clear straightforward language. We also employ a combination of the methods set out as follows below:

- We provide privacy information in a layered manner with a first layer of information offered via easy-to-read contextual notices, which provide information about privacy choices within the user interface. These contextual notices, sometimes called just-in-time notices, contain short, plain-language text to describe choices and visual cues to help users understand their options and to quickly move through their privacy choices during set-up.
- This first layer leads to our Microsoft Privacy Statement, which details Microsoft's data protection policies and practices in clear, straightforward language we believe a child could comfortably engage with.
- We also provide information about data collection, use, and controls as part of our privacy Dashboard. See Appendix 1 for an example of how Microsoft makes use of this approach.
- We provide further safeguards and controls for the responsible adult to promote online safety and responsible behaviours for children. This is a practical safety measure to permit parental supervision and control. We enable a range of privacy-protective settings which are made available depending on the age and capabilities of children such as family account features, which enables families to stay connected and allows parents set stricter privacy settings for children's accounts. These settings can help increase visibility around children's online behavioural habits and give options to parents to implement activity reporting, screen time limits, location sharing, and content filters for their children. See Appendices 2 and 3 containing examples of family protections on our Xbox platform.

- At Microsoft, we understand the increased risks when processing children's personal data. We do not deliver interest-based advertising to children identified as under 16 years of age in their Microsoft account. This advertising restriction is an effective example of privacy by design which enhances privacy protections for children.
- We implement content restrictions on Windows 10 and Xbox One devices to further enhance privacy protection for children. This includes settings to block inappropriate apps, games, and media (labelled as "Access to Content" on console); block inappropriate websites (labelled as "Web Filtering" on console); and require children to ask a parent before making purchases in Microsoft Store ("Ask a parent"). On Xbox One, we implement default settings for children below the age of 8 which block inappropriate apps, games, and media. See Appendix 4 for further details.

15. Do you think products/services that are used by or offered to children should have built-in default privacy settings that vary according to the age and evolving capacities of a child? For example, should there be stricter privacy settings for younger children? How should these variations in the privacy settings be given effect?

We believe a neutral user experience accompanied by clear, layered privacy information can serve as an effective way to deliver privacy protections to children. Children's privacy can be further protected and strengthened as appropriate to the age and capabilities of the child through parental engagement with the privacy-protective settings we describe in our response to Question 14 above.

16. Are there any other particular issues you would like to raise with the DPC in connection with the subject matter of this consultation?

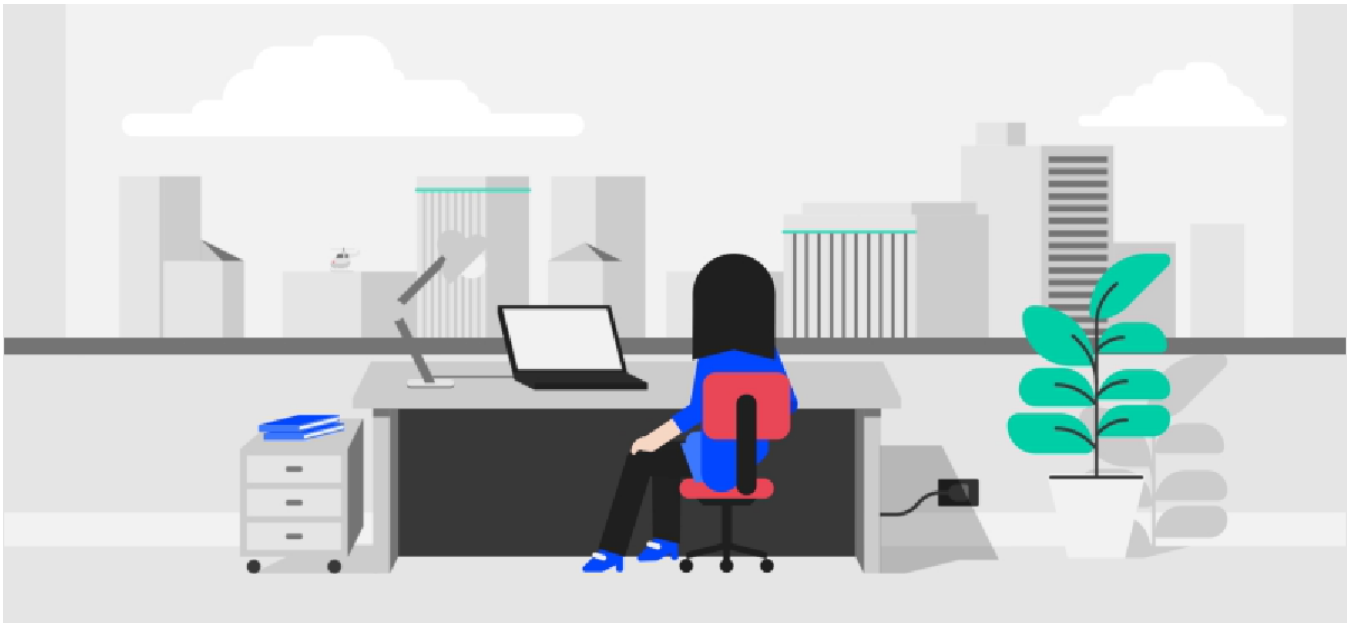
We are grateful for the opportunity to engage with the DPC on this public consultation and are happy to continue the conversation if helpful. We don't have further issues to raise at this time.

APPENDIX 1

What kinds of data does Microsoft collect?

Microsoft collects data to help you do more. To do this, we use the data we collect to operate and improve our software, services and devices, provide you with personalised experiences, and help keep you safe. These are some of the most common categories of data we collect.

Web browsing and online searches



Like many search engines, we use your search history and the history aggregated from other people to give you better search results. To speed up web browsing, Microsoft web browsers can collect and use browsing history to predict where you want to go. Cortana can make personalised recommendations based on your browsing and search history.

You can choose whether your browsing history is collected via the Feedback and Diagnostics Setting in your Windows privacy settings. You can also manage whether Cortana has access to your search and browsing history in Cortana and Microsoft Edge settings.

Manage your Bing search history

Learn more about browsing data and privacy

Read about web activity in the Privacy Statement

Places you go

Location information helps us give you directions to the places you want to go and show you information relevant to where you are. For this, we use the locations that you provide or that we've detected using technologies such as GPS or IP addresses.

Detecting locations also helps us protect you. For example, if you almost always sign in from Tokyo, and suddenly you're signing in from London, we can check to make sure that it's really you.

You can turn location services on or off for your device in Settings > Privacy > Location. From here, you can also choose which Microsoft Store apps have access to your location and manage the location history stored on your device.

To view and clear location data that's been associated with your Microsoft account, go to account.microsoft.com.

Learn more about Windows 10 and location

APPENDIX 2

Xbox Support

- Xbox One
  - Xbox & accessories
  - Password & security
  - Getting started
  - 4k and HDR
  - Apps
  - Console
  - Controllers
  - Ease of Access
  - Family
  - Networking
  - OneGuide and Live TV
  - Social and Broadcast
  - Microsoft Store
  - Voice and digital assistants
  - Warranty and service
  - Xbox Insider
- Xbox 360
- Xbox on Windows 10
- Games
- Mixer
- Billing
- My account

Family: Privacy protection

Trending topics | Privacy protection | Safety tools

Gaming and ratings | Family account | Social and broadcast

Definition of a Microsoft child account

Learn what a child account is and what qualifies a Microsoft account to be treated as a child account.

Benefits of creating a family on Xbox One

Learn about the benefits of creating a Microsoft account for every member of your family so that they can enjoy the Xbox experience.

How to add a child to a family account

Find out how to add a child account to a family account.

APPENDIX 3

Xbox Support

- Xbox One
- Xbox 360
- Xbox on Windows 10
- Games
- Mixer
- Billing
- My account
  - Error messages and codes
  - Gamertag and profile
  - Manage account
  - Password and security
  - Xbox Live membership
  - Warranty and service

Benefits of creating a family on Xbox One

Overview

By creating a Microsoft account for each person in your family, you can personalize each family member's online experience based on age-appropriate limits that you set. Those settings will apply to any Xbox One or Windows 10 device they sign in to.

Family-friendly Microsoft Store

- Easily add money to your child's Microsoft account, and set limits for how much your children spend in Microsoft Store on account.microsoft.com/family.
- Review your child's purchase history and the credit cards on your child's account.
- Set limits so when your children browse content in Microsoft Store, they'll only be able to see age-appropriate content.

Family settings for all Xbox One and Windows 10 devices

- Decide how each child interacts with others, shares their profile information, joins multiplayer games, or adds friends to their friends list by customizing the Xbox safety settings.
- Manage all content and web restrictions online at account.microsoft.com/family or on the Xbox One console.

Personalized play

- The visual experience on the dashboard can reflect each family member's personality. They can choose their own colors, select their own gamertag and gamerpic, and specify which apps they want to pin to the account home page.
- Everyone has his or her own achievements, gamerscores, and friends list that they can take with them when they use their profile at their friend's house or anywhere else.

APPENDIX 4

Set content restrictions on Windows 10 and Xbox One

Applies to: Microsoft account

Content restrictions help keep kids safer on Windows 10 and Xbox One devices and include settings to:

- Block inappropriate apps, games & media (labeled as **Access to content** on console)
- Block inappropriate websites (labeled as **Web filtering** on console)
- Require kids to ask a parent before buying stuff in Microsoft Store (**Ask a parent**)

Content restrictions can be set up on account.microsoft.com/family or on Xbox One. While content restrictions determine what kind of content your child can have access to, **screen time** determines how long they can use it, and when, but screen time limits can only be set up and managed on account.microsoft.com/family.

Set up screen time limits

Tip

After you've set content restrictions for your child, it's a good idea to turn on Activity reporting so you get weekly reports of their online activity. You can block or allow things right from the report. Go to account.microsoft.com/family and sign in with your Microsoft account, then find your child's name and select **Activity**.

Block inappropriate apps, games & media

Essentially, you set an age limit for content, and anything rated above it will need adult approval. On Xbox One, this setting is called **Access to content**, and we turn it on automatically if your child is under the age of 8. (By default, it's set to the age associated with your child's Microsoft account.) If they're over the age of 8, the default setting is **Unrestricted**, so it's a good idea to double-check it for your little gamers.

Block inappropriate apps, games & media online and on console

Block inappropriate websites

Help protect your child from surfing adult content on the web when they use Microsoft Edge and Internet Explorer browsers. (On console, we call this **Web filtering**.) We block many sites automatically,

but you can also block or allow specific sites, or choose to only allow your child to visit sites you've told us are OK.

Block inappropriate websites online and on console

Require kids to ask a parent before buying stuff in Microsoft Store

Turn on **Ask a parent** and require adult approval for the things your child wants to buy in Microsoft Store, except what they buy with gift cards or money in their Microsoft account. Of course, they'll still need permission if what they're trying to get exceeds the age limit for content that you have set—even when **Ask a parent** is off. Easily respond to your kids' requests to buy things through email or on account.microsoft.com/family.

Turn on Ask a parent online and on console

Tip

To keep track of what your child buys, go to account.microsoft.com/family and sign in with your Microsoft account. Find your child's name, then select **More options** > **Spending** to view purchase history and payment options, or put money in their Microsoft account.

Responding to kids' requests

Sometimes it's fun – or necessary – to break the rules. Your child may need something for homework, or you may want to reward them by letting them get the latest game everyone's talking about. You can respond to many of their requests through email, or if you share a device – say, a family Xbox One or Windows 10 PC – you can approve their requests on the spot. Of course, you can always respond to all requests anytime on account.microsoft.com/family.