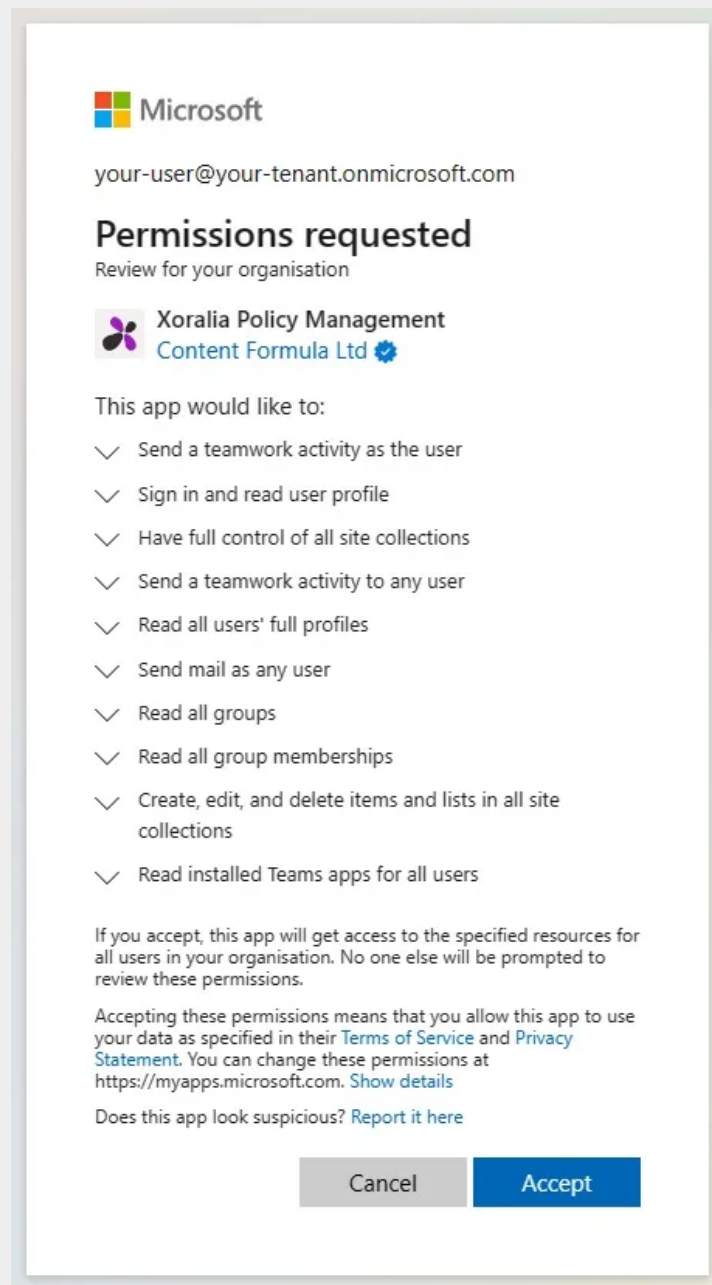



# How Xoralia accesses your information

Xoralia uses a Microsoft verified Entra ID Enterprise Application to communicate with your Microsoft 365 tenant. Our Enterprise Application uses a mix of delegated and application permissions, which we describe below.

During installation, you will be presented with a permission request like below. This details each of the permissions that Xoralia requires to carry out its operations. These permissions are not individually configurable and are required to be accepted by a Microsoft 365 Global Administrator (or Entra Administrator) for Xoralia to work correctly.




The screenshot shows a Microsoft permission request dialog. At the top, it displays the Microsoft logo and the user's email address: your-user@your-tenant.onmicrosoft.com. Below this, the title "Permissions requested" is followed by the instruction "Review for your organisation". The app being requested is "Xoralia Policy Management" by "Content Formula Ltd". The dialog lists 13 permissions that the app would like to access, each with a downward arrow icon. At the bottom, there is a warning about the scope of access, a link to the Terms of Service and Privacy Statement, and a "Report it here" link. Two buttons, "Cancel" and "Accept", are located at the very bottom.

 Microsoft

your-user@your-tenant.onmicrosoft.com

### Permissions requested

Review for your organisation

 Xoralia Policy Management  
Content Formula Ltd

This app would like to:

- Send a teamwork activity as the user
- Sign in and read user profile
- Have full control of all site collections
- Send a teamwork activity to any user
- Read all users' full profiles
- Send mail as any user
- Read all groups
- Read all group memberships
- Create, edit, and delete items and lists in all site collections
- Read installed Teams apps for all users

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [Terms of Service](#) and [Privacy Statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel Accept

Delegated permissions are a type of permission that requires a signed in user to be accessing the application and the operation will be performed on behalf of that user. For example, a delegated operation might be to view a list of files from a SharePoint site – Xoralia will perform this as a delegated query and will query that information as the logged in user, meaning it will only display information to the user that they have access to from that SharePoint site.

Application permissions are a type of permission that does not require a signed in user and will allow the Xoralia application to perform operational and service level tasks without user interaction. An example of this is a library synchronisation that Xoralia performs every 10 minutes to check for updates in SharePoint document libraries.

Xoralia requests the following Microsoft Graph permissions:

- **Send a teamwork activity as the user**
  - Type: delegated
  - Reason: Used by our Microsoft Teams app to send notifications to users
  
- **Sign in and read user profile**
  - Type: delegated
  - Reason: Allows the user to sign in to Xoralia and access information within Xoralia
  
- **Have full control of all site collections**
  - Type: delegated
  - Reason: Allows Xoralia administrators to associate libraries to Xoralia to which they have access. Also allows users to read documents within Xoralia to which they have access.
  
- **Send a teamwork activity to any user**
  - Type: application
  - Reason: Used by our Microsoft Teams app to send notifications to users
  
- **Read all users' full profiles**
  - Type: application

- Reason: Xoralia allows document owners to target documents to users. This permission allows Xoralia to view users inside of your Microsoft 365 tenant to know which users are to be targeted.
- **Send mail as any user**
  - Type: application
  - Reason: As a Xoralia administrator, you can set which email address should send notifications (such as must read and expiry notifications). This permission allows Xoralia to do that.
- **Read all groups**
  - Type: application
  - Reason: Xoralia allows document owners to target documents to groups. This permission allows Xoralia to view groups inside of your Microsoft 365 tenant to know which users are to be targeted.
- **Read all group memberships**
  - Type: application
  - Reason: Xoralia allows document owners to target documents to groups. This permission allows Xoralia to view groups inside of your Microsoft 365 tenant to know which users are to be targeted.
- **Create, edit, and delete items and lists in all site collections**
  - Type: application
  - Reason: Xoralia can create libraries and add meta data columns to associated libraries when an Xoralia administrator triggers that action. This permission allows that control – Xoralia will only ever create libraries when a Xoralia administrator requests so and will never use this permission for any other action. This permission is also used by the Xoralia sync process to update library and document information.
- **Read installed Teams apps for all users**
  - Type: application

- Reason: Allows Xoralia to find the Teams app inside of your tenant to send targeted notifications to users (such as Must Read notifications)

You can limit who can access Xoralia by going to Enterprise Applications within Microsoft Entra ID and opening the Xoralia Policy Management app. Once you have this open, select properties and enable the 'Assignment required?' option. Save this property and open the 'Users and Groups'. With this setting enabled, only users and groups listed here will be able to access Xoralia. Add your users and groups here using the 'Add user/group' option.