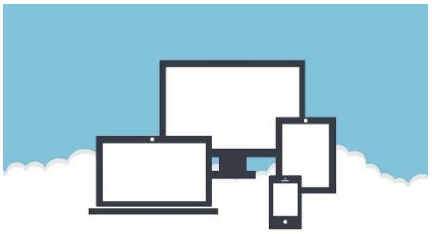
Guidance on Facebook Pages, Groups and use of the ‘like’ button on your Website.



If you want to expand your school communications online in a place where students and parents are already spending a lot of their time, it makes sense for you to consider Facebook. While Facebook Groups are not a replacement for password protected Portals within your website, you may find that they are a useful additional communication tool for your school.

However with so many users, Facebook is a target for scams. It can expose the personal information the School holds far beyond connected friends, and you should think carefully before jumping into using it.

The following are good things to consider when weighing up the risks versus the benefits for your school.

What are the Security Risks?

Facebook have widely known security concerns over how they handle, protect and share personal information.

Facebook conducts web tracking on users even when the app is not in use, they also use algorithms to aid targeted marketing use. Facebook also uses Artificial Intelligence (AI) and machine learning to detect “bad” content before anyone reports it, this content then gets reviewed by humans so there is a potential for a data breach occurring if it contains personal information.

In theory, new Facebook security features provide protection against scams and spam, but unfortunately, they’re mainly ineffectual. These could easily get posted on your Page or Group if approved and affect your users.

What kind of Scams?

Facebook scams tap into interest in the news, holiday activities and other topical events to get you to innocently reveal your personal information. Facebook posts such as "In honour of Father’s Day" seem harmless enough, until you realize that information such as your children’s names and birthdates, pet’s name and street name are now permanently on the Internet. Since this information is often used for passwords or password challenge questions, it can lead to identity theft.

Other attacks on Facebook users include "clickjacking" or "likejacking". This malicious technique tricks web users into revealing confidential information or takes

control of their computer when they click on seemingly harmless webpages. One disguise is a button that appears to perform another function. Clicking the button sends out the attack to your contacts through status updates, which propagates the scam. Both clickjacking scams take users to a webpage urging them to watch a video. By viewing the video, it's posted that you "like" the link and it's shared with your friends, spreading it virally across Facebook.

What is the difference between a Facebook Page and a Group?

Pages: Pages are a public and brilliant way of promoting your school to a wider audience. It can be searched, and any content posted can be viewed. Imagine it as a front facing advertisement window for your school. It contains and collects analytic data (cookies) so you can see when your audience is most active, post engagements, schedule and host advertising tools. You can't interact or see details of individuals outside of your posts.

Groups: Facebook Groups can be affiliated with Pages, so that a Group is displayed on the Page and clearly associated. However, you need to be fully aware of your group's privacy settings and who can access the information you post there. There are two privacy methods available:

- **Public** – meaning anyone can join, see who's in the group and what they post. DO NOT post personal data in these groups unless you have consent to do so.
- **Private (closed)** - meaning only members can see who's in the group and what they post. There are also options where people can request to join a group and administrators can approve if they are accepted. If a user interacts with the group, it won't also show in their friend's newsfeeds. You can post personal data in these groups if all members are entitled to see it.

Facebook lets Groups publish rules to avoid unexpected issues with problem posts. Be sure to put those in place and publish them on your page before you launch, and ensure you have a set policy in place for social media use.

Use Facebook administrator tools to delete inappropriate comments, ban Code of Conduct violators, or even turn off commenting for a post if the subject gets too heated.

What do I need to put in place when I set up a Page or Group?

For both Pages and Groups:

- Complete a DPIA to ensure that you have identified all risks associated with the use of this new technology and sharing of personal data. You can find a template and guidance for this on the Veritau Portal here.

Veritau
Assurance Services for the Public Sector

- Identify your legal basis for putting personal data on the page or group. This is likely to be either Legitimate interests (in the interests of the school to market itself) or consent (both for the use of cookies and personal information). Legitimate Interest and consent will always be used on pages. Please contact Veritau if you need advice on this and conducting the legitimate interests test.

- Update your Asset Register to add Facebook as a data processor (groups) or joint controller (pages).

- Allocate a dedicated Social Media administrator to ensure that the page is monitored and anything inappropriate is shut down, for example a parent openly discussing a bullying case.

- Don't use private accounts to set up Facebook Pages or Groups. Set up a generic account for the school.

- Use Facebooks guidance on Groups and Pages to get them set up.

- Carefully consider what personal data will be put on Facebook Groups. Always consider if there is a more secure way to share the information.

- Adopt a Social Media Acceptable Use Policy (the Veritau Acceptable Use Policy on the portal included this section for adaptation) that clearly defines roles and responsibilities, how you will monitor posts, how you will handle removal of posts, how you will manage enquires relating to data subjects' rights (subject access requests, requests for erasure of data, etc) received over this platform.

- Ensure your Privacy Notices (e.g. pupil and parents, website) are updated to reflect this use of people's data and cookies.

For Facebook Pages:

- You are a Joint Controller with Facebook and have more responsibility and liability. Ensure that you thoroughly read the Policy Addendum here.

- Create a Specific Privacy Notice for that Page and upload it onto Facebook (see Facebook's Policy Addendum (and addition to their main policy)). It must contain the following:

    - How and why you are processing personal data
    - Your legal basis for each type of data processing activity
    - A Joint Controller statement
    - Details of your legitimate interest test assessment
    - Who you will be sharing data with (including Facebook)
    - If you will be transferring data overseas

Veritau
Assurance Services for the Public Sector

    - Details on use of cookies (and consent)
    - Details of how you will handle data subjects' rights

- Ensure your School's contact information is accurate on the page's "about" page, so people can contact you regarding the use of their personal data.

- You need to ensure you are able to report data subject rights requests (subject access requests, requests for erasure, etc) regarding insight data to Facebook within 7 days and via their online form.

For Facebook Groups:

- Ensure that your Group privacy settings are applied.

- Consider how you will obtain Consent. Consent to receive targeted communications through the group is accepted when they become a member, i.e. on a parents' forum putting out information about the upcoming charity fundraiser. They must apply to join the group, you can send them an email from the group suggesting they join but you should never add users without permission.

- If members joined the group prior to GDPR being implemented in May 2018 remove them from the group and ask them to apply to re-join, this will show they have given consent.

- Consider how you will authenticate members of your group, are they real parents/students - or even real people? You should add some authentication questions for them to answer to confirm identity to join the group.

- Don't add any non-school Facebook Pages to your Group as any administrators of that Page can view and interact with that group.

- Don't add a third-party app to the group as they can access posts and comments made but not see who wrote the posts/comments unless the author has given that app permission.

- Put your rules up regarding acceptable use of the group under "About this group". As part of the application process you can have a question asking them to confirm they will abide by the acceptable use rules.

Using the Facebook Like button on your Website

If you use the Facebook Like button on your website, this provides Insight data (cookies) that transfers to Facebook and as such you are a Joint Controller with Facebook (see "Facebook Page Legal Responsibilities" in this guidance) This is because you are sharing data with Facebook without consent via cookies. This would also be applicable for LinkedIn, Twitter etc.

You must have a cookie consent banner on your website that details what cookies are being used, this must be linked to your cookie/website privacy notice which details what information is being collected and who it is shared with.

You also need to ensure that if someone does not consent to the use of the Facebook like button that your website provider has prevented the information being sent to Facebook by that user. Guidance for your provider can be found at https://developers.facebook.com/docs/facebook-pixel/implementation/gdpr/

If you have any third parties who embed content in your website you will need to check what plug-ins/widgets are collecting data and record it (i.e. google analytics). You will need to ensure that they do not automatically transfer data prior to collecting consent from the user. Speak to your IT/website provider for assistance with this.

You will need to update your Website Privacy notice to reflect your status as a Joint Controller with these applications.

What are your and Facebook's Legal Responsibilities?

As a Facebook page both you and Facebook are responsible and accountable for complying with GDPR for insight data (information about visitors e.g. what pages they are visiting). Facebook have provided a Page insights Controller Addendum here.

The Court of Justice of the European Union determined that for insight data Facebook Page admins (in this case, the school) are **Joint Controllers** with Facebook.

A Data Controller is someone who decides **why** and **how** personal data is processed – you are responsible for the data and liable for any risks to it.

Joint **controllers** are "two or more controllers [who] jointly determine the purposes and means of processing." Joint controllers can **decide between themselves** who takes responsibility for complying with which of the various obligations under the GDPR and other privacy laws.

Facebook specifically says it will take care of the duties covered by the following GDPR Articles (you will also as the Page Administrator have some duties under these articles):

- They will provide information to Facebook users about what information they collect, how it is processed and who they share it with.
- They will comply with data subject's right of access.
- Facebook will have Security embedded, and provide options for settings to be tailored.

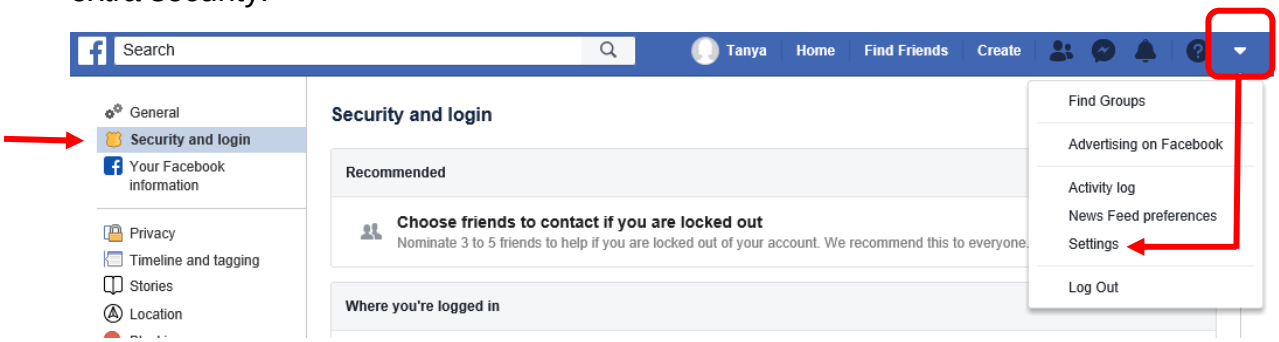
Facebook also makes it clear that although Page Administrators are joint controllers, Facebook will be responsible for the processing of Page Insight data and as such any data subject rights requests received **specifically regarding insight data** must be reported to Facebook within 7 days of receipt using their online form.

Guidance on Account setting for using Facebook Accounts, Pages and Groups

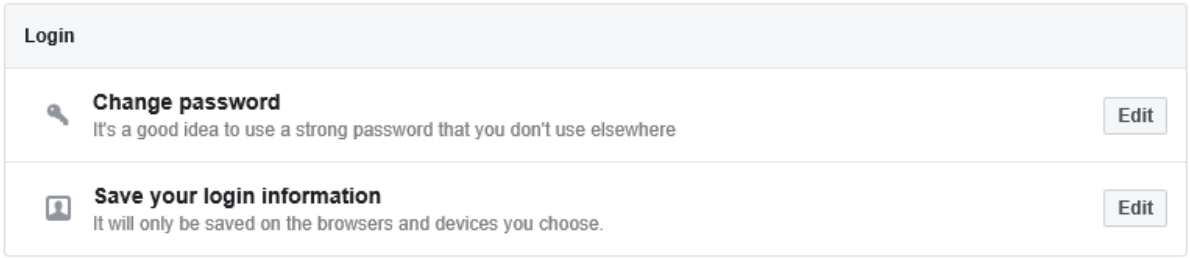
Below is some guidance on settings that you need to check and consider applying to assist with keeping your Facebook account, Page or group secure. There are also additional options that you can consider dependant on how you wish your Page/group to function that have not been covered below.

Generic Facebook Account security settings

If you have not already, create a new generic Facebook account to be used by the School using a school email address. Ensure that you go into settings and add extra security.



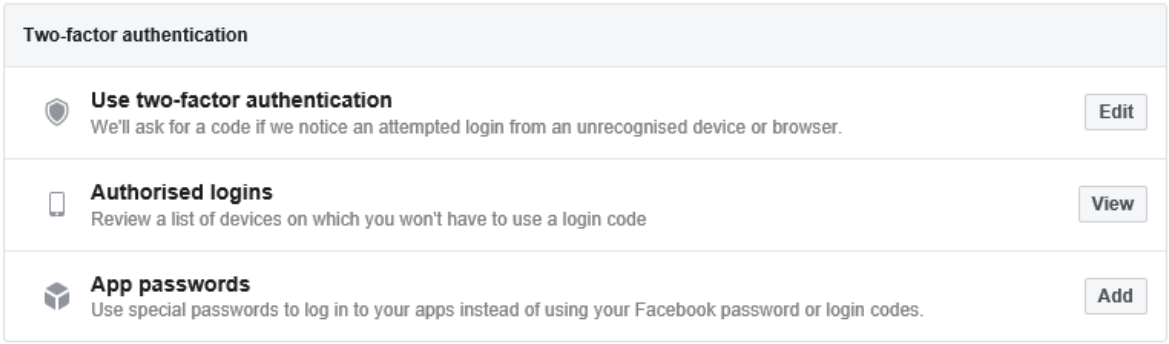
Under Login



- **Change password**. Ensure that if you hand over account administration you Change the password.
- **Save your login information**. This is used to prevent Facebook automatically logging in on a device. Select 'Remove account' this will ensure that when you next open Facebook on an authorised device it will ask for both your email address and password.

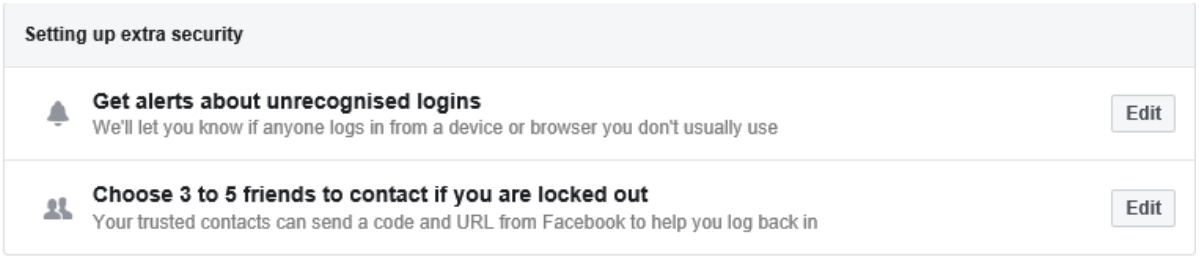
Veritau
Assurance Services for the Public Sector

Under Two-factor authentication



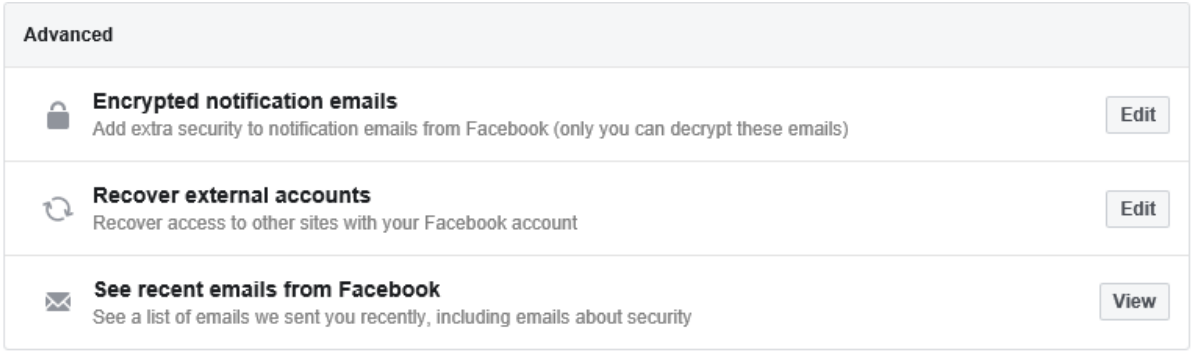
- **Use two-factor authentication.** Edit this to help protect your account. This will add an extra layer of security to prevent the account being accessed without authorisation by an unrecognised device or browser. The best option would be to use an authentication app i.e. Windows Authenticator which can be used to generate a code.
- **Authorised logins.** This will display a list of devices that have been authorised to login to your account without a code (see two factor authentication above). Review this regularly and ensure that devices that should no longer have access are removed.

Under setting up extra security



- **Get alerts about unrecognised logins**. Turn this on to be alerted to unexpected logon action on this account. This can be set to be sent via notification, messenger, and email to the address set up or you can add a new email/mobile number.

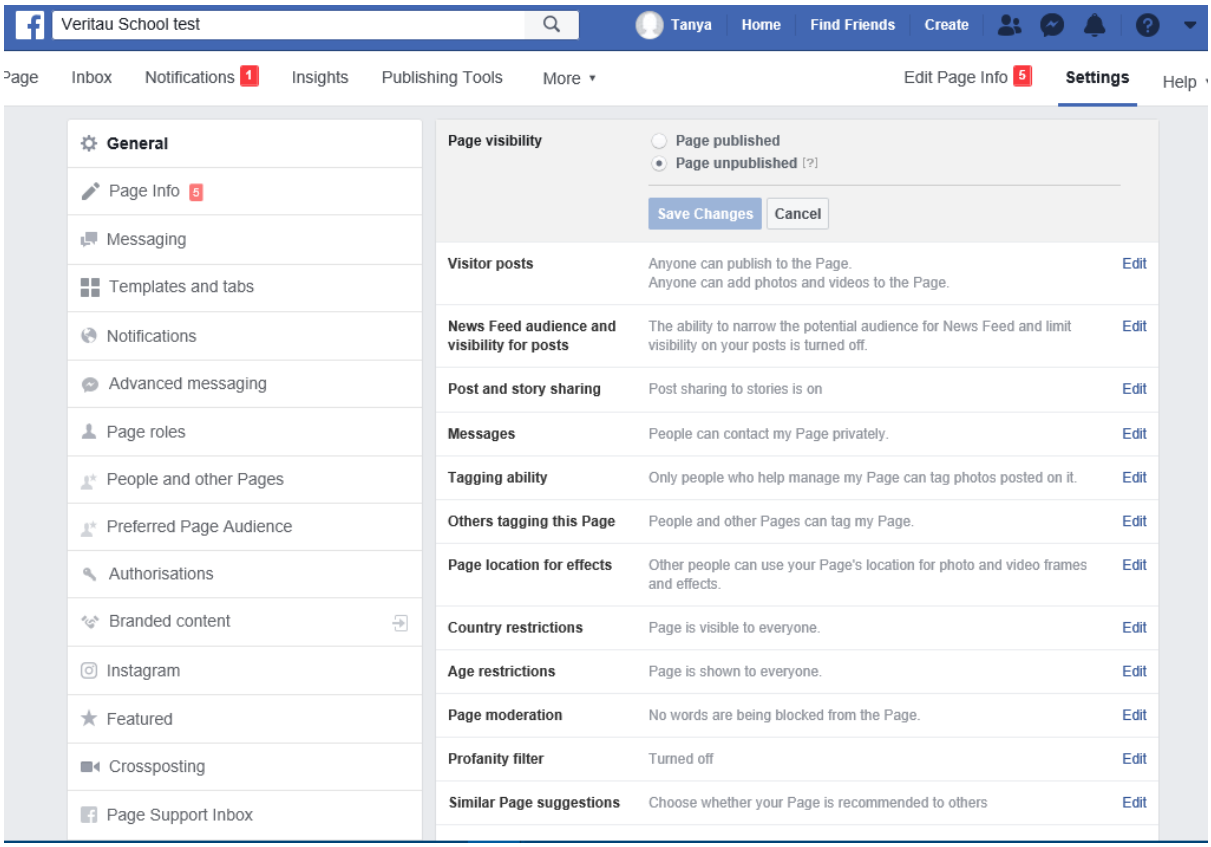
Under advanced



- **See recent emails from Facebook**. You should regularly check this area as it shows the recent emails from Facebook that have been sent to you, particularly those about security.

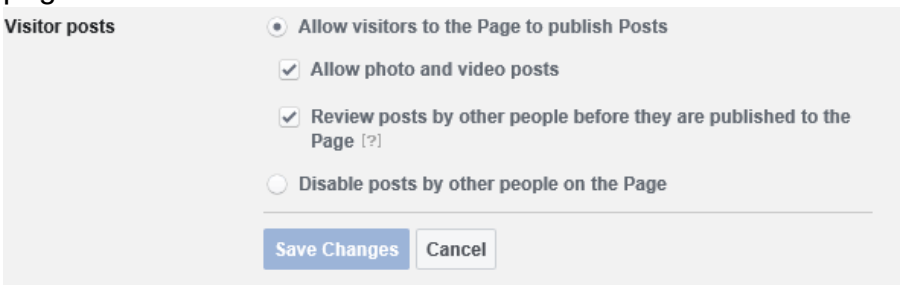
Facebook Page security settings

If you have a Facebook Page set up, then you can use the following settings to enhance your security, using settings the option page will look like this:



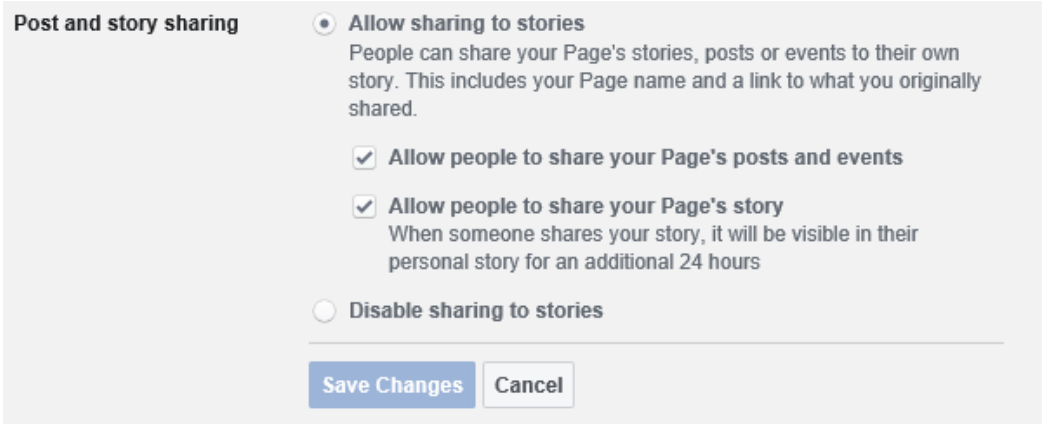
<u>General Settings</u>

- **Visitor posts.** Ensure that you select Review posts by other people before they are published to the page. This will ensure that you get the opportunity to review what content appears on the page. You can also disable photo and video posts from visitors, or disable any posts from others appearing on your page.

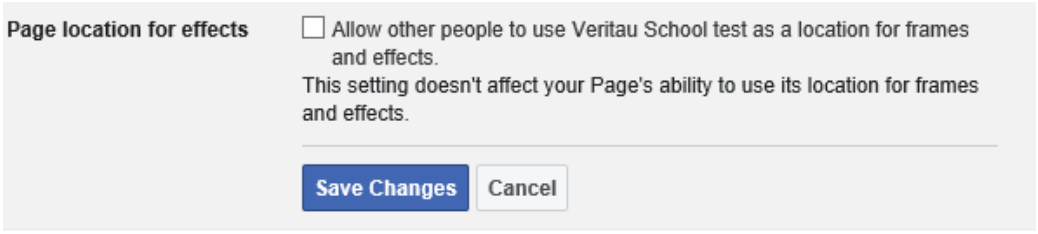


Veritau
Assurance Services for the Public Sector

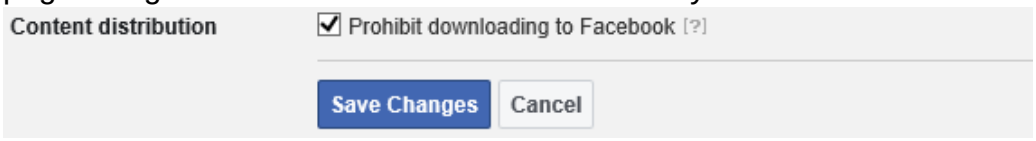
- **Post and story sharing**. You can tailor your options here to prevent your posts being shared. You will need to determine which option your school wants to use.



- **Page location for effects.** You should deselect this option as it prevents misuse of your logos, photos and content by users.



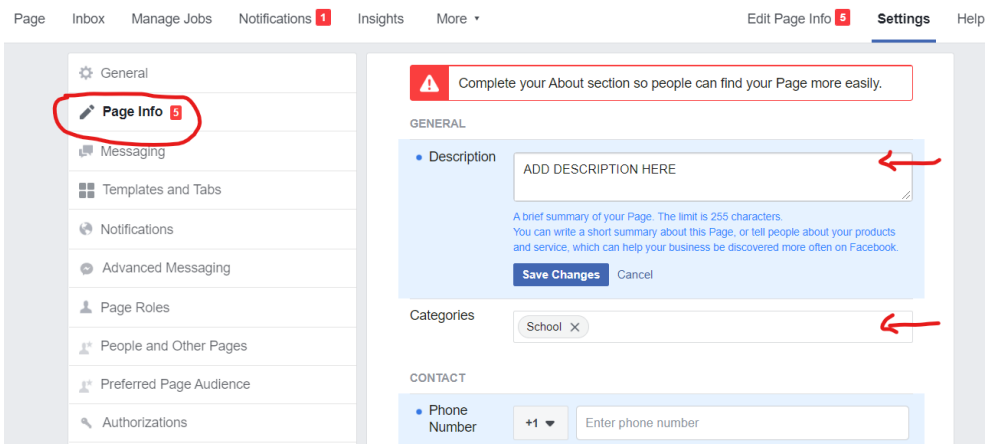
- **Content distribution.** Select the box to stop any videos you put on your page being downloaded and further distributed by users.



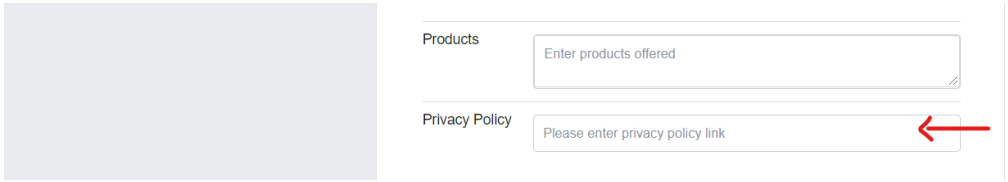
Page info

Under Page Info you must add a brief description of your page, add a category and upload your privacy notice link that is applicable to this page. You must determine yourself what other fields need completion.

Veritau
Assurance Services for the Public Sector

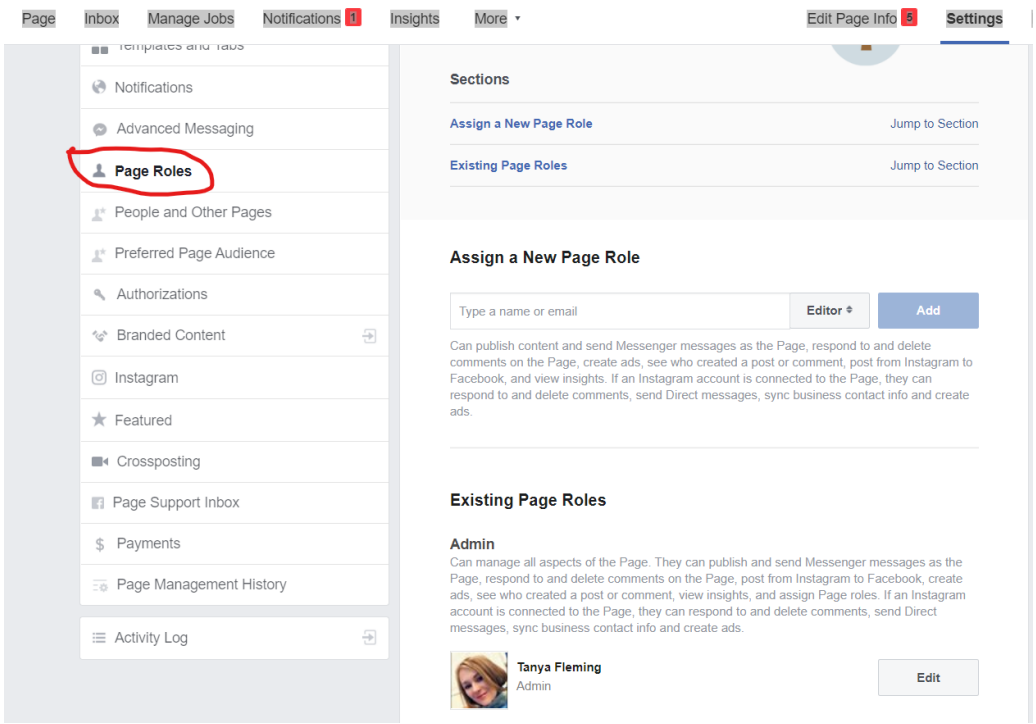


Scroll down to bottom



Page roles

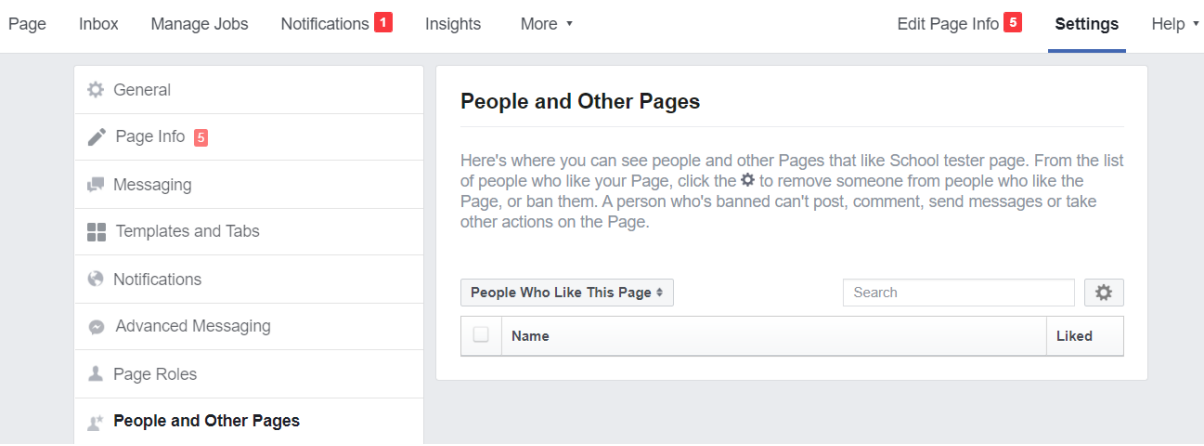
This is where you review who are the page administrators, or editors. You need to regularly review these and remove those with inappropriate access.



People and other Pages

If you need to block a person or page from being able to post comment or send messages this is where you would add their details.

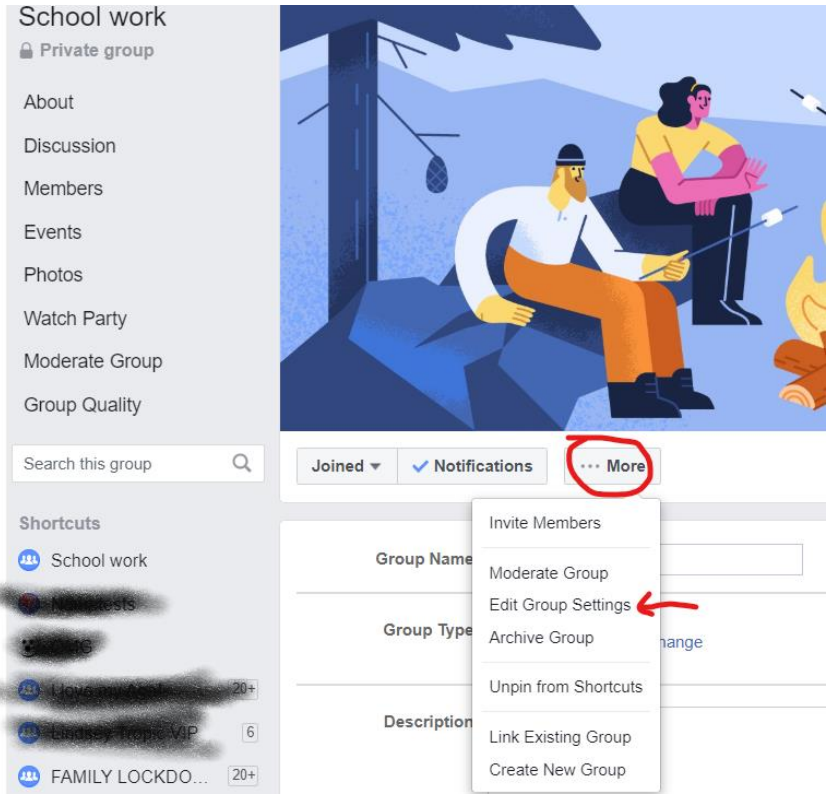
Veritau
Assurance Services for the Public Sector



Facebook Group settings

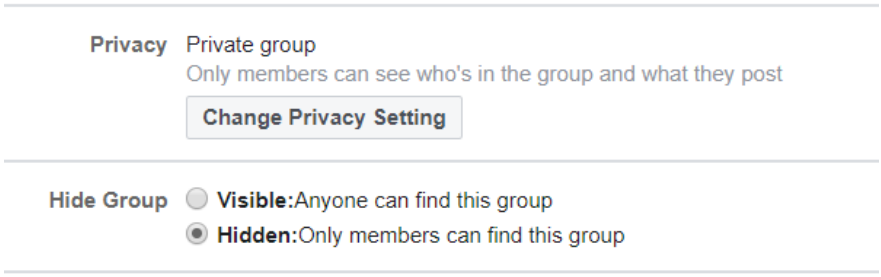
Navigate to your Group page once set up as the administrator.

If you need to change the privacy setting of your group to Private or Hidden this can be done under edit group settings.

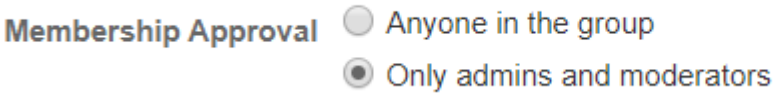


- **Privacy.** Change the setting here to make the group private so only members veiw posts.
- **Hide group.** Select if you want the group to be visible or Hidden

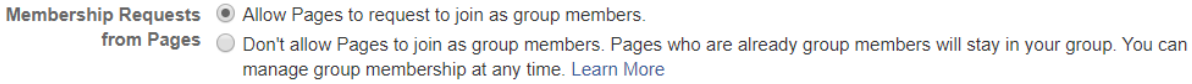
Veritau
Assurance Services for the Public Sector



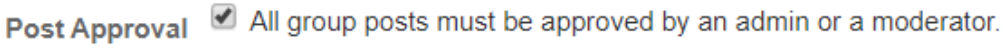
- **Membership approval.** Set this to only admins and moderators.



- **Membership requests from Pages.** Ensure that you have selected don't allow pages to join as group members.



- **Post approval**. Ensure this is ticked to ensure all posts have to be manually approved by an admin.

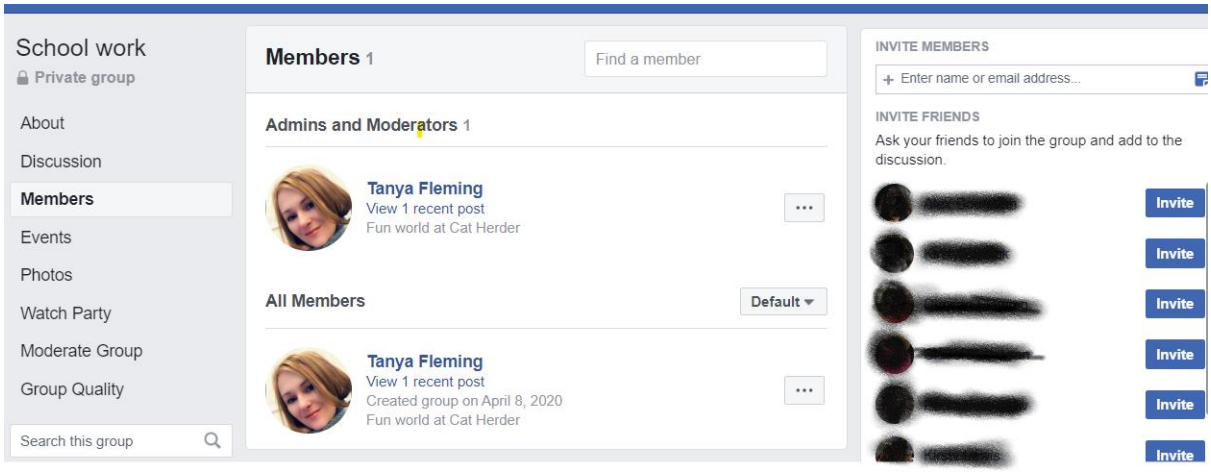


<u>Under Members on your group page</u>

You should regularly review who your members are and who are admins and moderators. You should ensure that you remove users who should no longer have access.

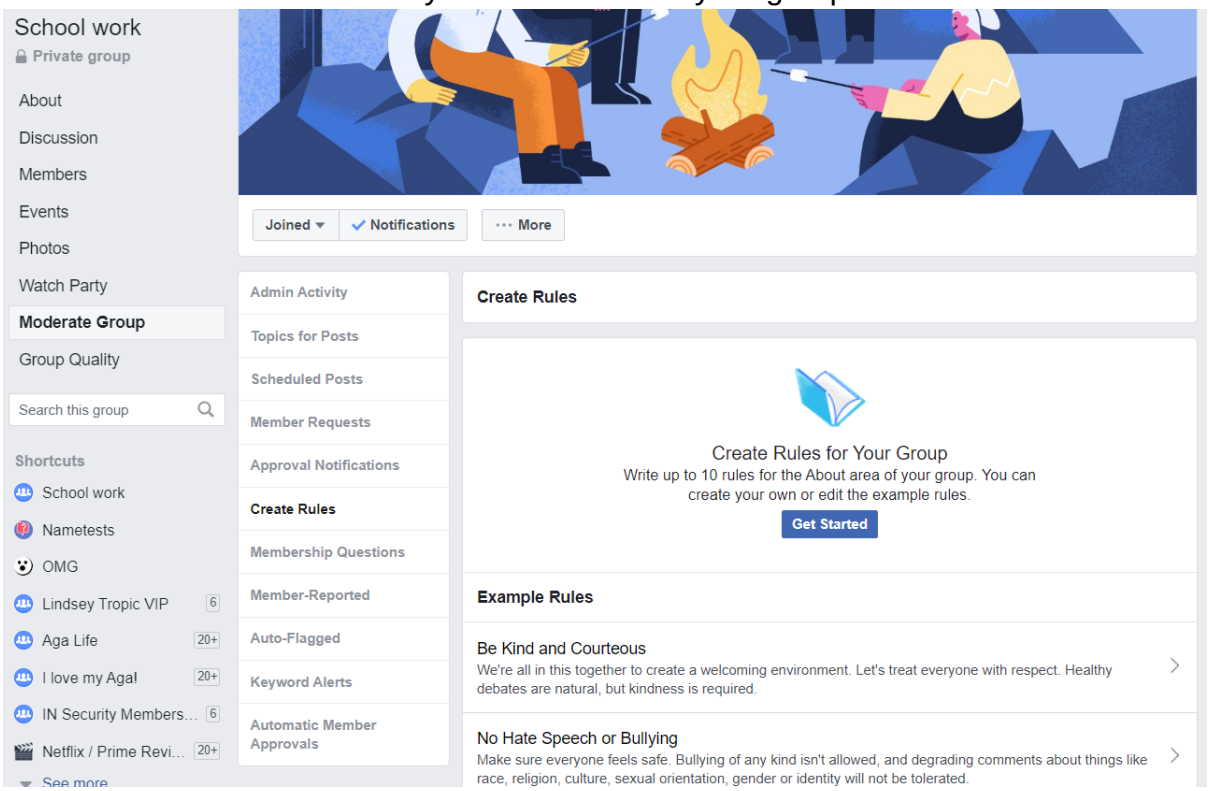
You can invite people to join your group via email or Facebook profile name (if known) by using the invite member's function on the right.

Veritau
Assurance Services for the Public Sector



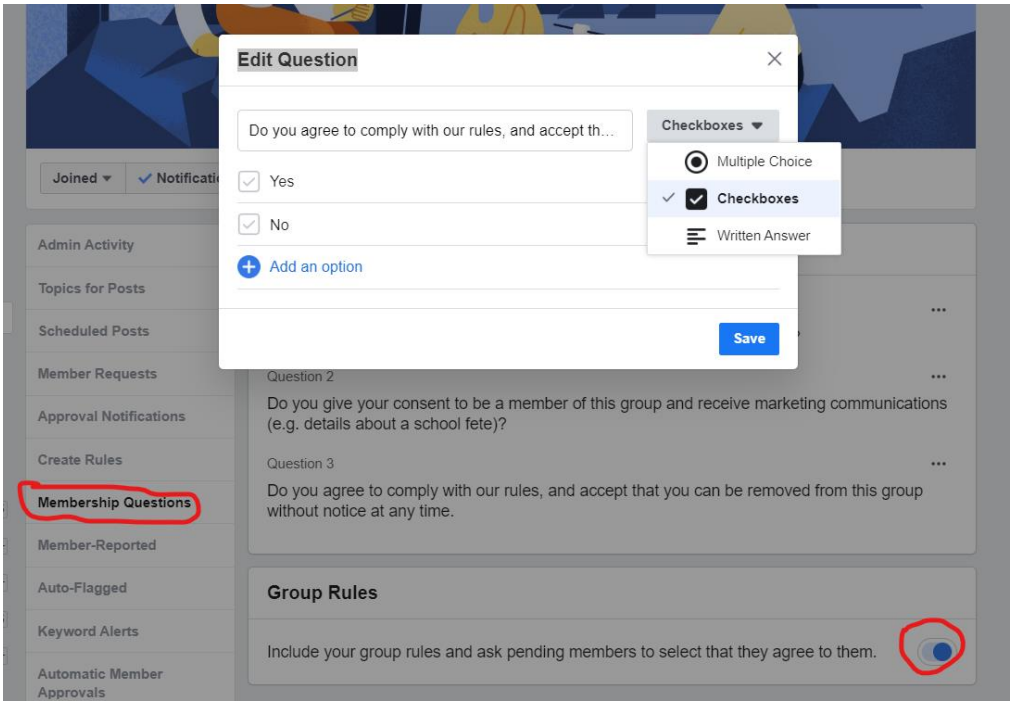
Under Moderate Group on your group page

- **Create rules**. This is where you customise your Rules for this page, you will need to determine what rules you want to set for your group.



- **Membership questions.** Use this to set questions that a person has to answer when applying to join your Group. You can tailor their response to be text, Multiple Choice or checkboxes. Some example questions are below and you should include a question that verifies that they are linked to a child. If you use a checkbox and provide both YES/NO options then this can be used to prove they have consented receiving marketing. Ensure you enable the Group rules function.

Veritau
Assurance Services for the Public Sector



- **Automatic Member Approvals, or preapproved memberships.** Ensure that you **don't** enable this option, you need to ensure that you have checked and approved applications to verify they are legitimate.

Veritau
Assurance Services for the Public Sector