# The Importance of Managing your Social Media Privacy Settings

Social Media is an integral part of our lives where we can share a wealth of information about ourselves on platforms, however they are privacy risks which you should be aware of as well.

There can be a tendency with some Social Media users, to overshare personal life details with family members, friends and co-workers in an effort to feel connected to them. This may seem perfectly innocent and without consequence, however these private details can unfortunately be used by identity thieves or other individuals with malicious intent.



# General advice on protecting your privacy on Social Media

* Create a unique, strong password which takes advantage of [two-factor authentication](https://en.wikipedia.org/wiki/Multi-factor_authentication) (when possible)
* It’s a good idea to be selective on your ‘friend’ on Social Media platforms, especially if you don’t them even if you’re using the platform for business networking
* When you create an account on any Social Media platform, one of your first actions should be to view the site’s privacy policy page and view any privacy settings, security or administration options. This page should also cover relating to what data of yours is shared, where it’s shared to and with whom
* Be mindful, that anything that is published online is never truly private, always consider your audience whenever you post something online



# Facebook



Within the UK, Facebook has a user base of 30 million people and the platform enables people to connect with family, friends, post updates, “check into” locations, send private messages (PM), join specific communities and upload images/video. Users of this platform can share the following personal information like their birthdate, hometown, and activities along with “tag or tagging” (identify) themselves and other friends in media uploaded. Facebook can be accessed on mobile devices via the app and desktop computers.

It’s worth remembering certain information within Facebook will be available to the public, including your name, gender, both cover and profile picture, networks, username along with your user ID.

Facebook has four options relating to types of audience, they’re:

* **Public** – This effectively means global access, anyone on or off Facebook
* **Friends** – Only people within your friends list on Facebook can view material
* **Custom** – Enables you to share or exclude content from specific individuals and lists
* **Only Me** – Content is restricted, so only you can view it

**Please click on the link below to view Facebooks' official guidance and tutorials on online privacy and settings.**

[Follow this link to view Facebooks' Privacy Settings and Tools (link opens in a new browser window)](https://en-gb.facebook.com/help/325807937506242)

# Twitter



Within the privacy settings, you can ‘protect’ your tweets, meaning they are private and only those who follow you on Twitter can view them. You should avoid including your location when you’re Tweeting, this provides an extra level of protection should be travelling or away from home for a prolonged period of time. Another setting that can be adjusted within the privacy settings is to allow only select people to tag you in photographs, this will again cut down on your location being shared.

Below is a summary of what features a ‘private’ account in twitter enables

* Only Twitter users approved by you may follow/subscribe and view your tweets
* Any Tweets you made in the past will be hidden from the public, and can only viewed or searched by approved followers
* Any Tweets you make will no longer appear in google searches or be “retweeable”
* Unless you send them to approved followers, any @replies you make will not be seen

Below are two other sections that should be considered or viewed when dealing with your privacy within Twitter

* The “passwords” section within twitter, lets you change your password.
* The settings within “Apps”, enable you to view what apps are connected to your account and ‘revoke access’ if you want

**Please click on the link below to view Twitters official guidance on online privacy and settings.**

[Follow this link to Twitters' Privacy advice (link opens in a new browser window)](https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public)

# Instagram



As seen in other Social Media platforms, the default setting for your profile and content you upload is set to ‘public’, meaning everyone (even those without an Instagram account), can view what you’ve uploaded. Settings can be adjusted so only approved followers can view whatever you post to Instagram.

**Below is summary of what can be adjusted within the privacy settings:**

* Adjust settings for photographs of you: This setting lets you automatically add photos others add you in or manually add them, if you would prefer to review them first
* Adjust Story Settings: You have the following options in relation to Instagram stories, you can hide them from specific people, enable message replies, allow your stories to be shared and choose whether to save or share you stories on other Social Media Platforms, i.e. Facebook
* Edit and Change your password and set up two-factor authentication (if you wish)
* View any blocked users (you can also block any new users as well)
* Make your account private: A person has to make a request to follow you in order to see your Instagram photos and stories
* See what accounts your Instagram is linked to: this lets you see what Social Media platforms, i.e. Twitter, Facebook your Instagram account is connected to

*There’s also the opportunity to review Instagram’s privacy policy within this section as well.*

**Some other privacy factors you may want to consider are listed below.**

Please remember, that any Instagram user will be able to read your bio and send you a photo or video direct to you, regardless of your privacy settings.

If you do decide to keep your Instagram access set to public, then please remember your phone’s **geo-location software** pins every photo you take with a location. It may be tempting to show off your latest holiday location but remember everyone will be able to see this information if your account is set to public. Before posting a photography, you do have the option to ‘**Add to your Map**’, it is advised this option is switched ‘**Off**’.

**Please click on the link below to view Instagram official guidance on online privacy and settings.**

[Follow this link to Instagram’s' privacy settings and Information (link opens in a new browser window)](file:///C%3A%5CUsers%5Cgregw%5CDownloads%5CFollow%20this%20link%20to%20Instagrams%27%20privacy%20settings%20and%20Information%20%28link%20opens%20in%20a%20new%20browser%20window%29)

# LinkedIn



There are a number of options within LinkedIn that enable you to control your account, privacy, what adverts you see and communication.

The account settings let you control your password and set up a two-factor authentication (if you wish). You should investigate the “Partners and Services” section as this will let you see who you’ve shared access to your LinkedIn account with and who can access your LinkedIn Data. You can stop sharing data with organisations and services any time, by clicking ‘Remove’.

Within the ‘Privacy’ settings you can select how others see you and how LinkedIn uses your data. The default settings within LinkedIn display your name, profile picture and headline will appear to anyone whose profile you view, however you can choose to be anonymous or only reveal specific information about yourself, e.g. the sector you work in. Another setting you may want to examine is around your connections. You can choose to share your connections with 1st –degree connections only or keep them completely private. Finally, you can control access to whom sees your profile picture, this can be restricted to 1st-degree connections, your entire network or all of LinkedIn. For security reasons it may be the best option to consider making your profile picture available to your 1st-degree connections.

Please click on the link below to view LinkedIn official guidance on online privacy and settings.

[Follow this Link to view LinkedIn Help - Managing your Account and Privacy Settings – Overview (link opens in a new browser window)](https://www.linkedin.com/help/linkedin/answer/66/managing-your-account-and-privacy-settings-overview?lang=en)

# WhatsApp



Students at UofG, have been known to set up study or social groups using WhatsApp, however, as with any platform you should be aware of the privacy settings and what data of yours is being shared via the App.

By default, WhatsApp privacy settings enable any WhatsApp user to see your last seen profile image and status. You should consider adjusting this under the privacy settings. Another default feature, you may want to adjust is WhatsApp shows your contacts when you last opened the App.

**Below is a list of profile areas that can be adjusted in the privacy settings**

* Last Seen
* Profile Photo
* About
* Status
* Live Location

The above have three viewing options associated with them, everyone, my contacts and nobody. Out of the above profile areas, you should consider setting ‘Live Location’ to ‘Nobody’ as this effectively allows users to track your GPS location. You may wish to adjust ‘Last Seen’ as this can also potentially reveal your location.

Under your ‘Account’ section, there is the option to set up a two-factor authentication, which again you should consider doing for security reasons.

[Follow this link to view the WhatsApp advice on privacy settings (Link opens in a new browser window)](https://faq.whatsapp.com/general/security-and-privacy/how-to-change-your-privacy-settings?category=5245250)

# Know who your friends/followers are

Even if all your privacy settings are carefully locked down, this doesn't mean you can safely post without thinking first. One of your friends/followers could take a screenshot of your post and share it more widely without your consent. This means it's really important to:

1. Regularly review your friends/approved followers if you are posting more personal information
2. Make sure you don't post anything what you wouldn't want certain people to see

