

Bebington High Sports College Co-operative community trust



This guideline has been taken from Safer Working Practice for Adults who work with Children and Young People in Educational Settings.

Communication between students and adults, by whatever method, must take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults must not share any personal information with a child or young person. They must not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults must ensure that all communications are transparent and open to scrutiny.

Adults must also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They must not give their personal contact details to students including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

This means that adults must:

- ***ensure that personal social networking sites are set at private and students are never listed as approved contacts***
- ***never use or access social networking sites of students.***
- ***not give their personal contact details to students, including their mobile telephone number***
- ***only use equipment e.g. mobile phones, provided by school/service to communicate with children, making sure that parents have given permission for this form of communication to be used***
- ***only make contact with children for professional reasons and in accordance with any school/service policy***
- ***recognise that text messaging must only be used as part of an agreed protocol and when other forms of communication are not possible***
- ***not use internet or web-based communication channels to send personal messages to a child/young person***

Social Networking Guidelines for Staff

The past few years have seen a dramatic rise in the popularity of social networking sites (such as Facebook, Flickr, Twitter) which offer a variety of ways to keep in contact with friends and relatives.

However, all users, especially those in education, must be aware of the security implications that these sites present.

This guide is aimed at raising awareness of how information can propagate through social networking, the steps you can take to protect yourself and the risks of certain types of conduct.

Facebook Concepts

Facebook is simply a tool that allows users to share information with other Facebook users. This information can take many forms, such as:

- Photographs
- Status updates (what you are currently doing / thinking)
- Movies
- Emails
- Forum posts

Users of Facebook can choose who to share this information with, such as:

- 'Only Friends' - other users who you have confirmed as a friend on Facebook
- 'Friends of Friends' - Users who are not necessarily *your* friend
- 'My Networks and Friends' - networks are groups you have chosen to join
- 'Everyone' - all users of Facebook



Friends are users who have sent a request (via Facebook) asking that you add them as a Friend. They are only classed as friends once you have accepted their request.



Remember that anyone can join a **Network**. You may be a member of the Network/Group '**I like cheese**', but students could have added themselves to that Network/Group as well

You can also specify individual friends and networks or groups.

From this simple concept, it is easy to see how information could be seen by other users who you would not usually wish to access it.

Basic Facebook Security

Facebook allows users to configure security setting to reduce the risk of personal information being accessed by unauthorised users. This can be done from the **Privacy Settings** menu:

Privacy Settings

From the Facebook menu choose **Settings** and **Privacy Settings**:



This will present the following screen:

- Privacy**
 - Profile** ▶ Control who can see information on your Profile page.
 - Search** ▶ Control who can search for you, what they can see and how they can contact you.
 - News Feed and Wall** ▶ Control what recent activity is visible on your Profile and on your friends' home pages.
 - Applications** ▶ Control what information is available to applications you use on Facebook.

<p>Block People</p> <p>If you block someone, they will not be able to find you in a Facebook search, see your Profile or interact with you through Facebook channels (such as Wall posts, Poke, etc.). Any Facebook ties you currently have with a person you block will be broken (for example, friendship connections, Relationship Status, etc.). Note that blocking someone may not prevent all communications and interactions in third party applications, and does not extend to elsewhere on the Internet.</p> <p>Block email address</p> <p>If you cannot find someone to block, you can block an email address. We will block any account associated with this email address currently or at any time in the future.</p>	<p>Block List</p> <p>Lisa Corlett (Manchester) (remove)</p> <p>Person</p> <p><input type="text"/> <input type="button" value="Block"/></p> <p>Email</p> <p><input type="text"/> <input type="button" value="Block"/></p>
--	---

From here you can access two of the most important privacy control pages on Facebook, **Profile** and **search**.



The following descriptions present only a basic overview. An exhaustive description would require hundreds of pages. You must use this guide and common sense to determine the appropriate levels of security

Profile Menu

From here you can choose who may access your information on Facebook.

[Privacy](#) ▶ [Profile](#)

Basic **Contact Information**

Control who can see which sections of your Profile. Visit the [Applications](#) page in order to change settings for applications. Visit the [Search Privacy](#) page to make changes to what people can see about you if they search for you.

See how a friend sees your profile:

Profile	Only Friends	[?]
Basic Info	Only Friends	[?]
Personal Info	Only Friends	[?]
Status and Links	Only Friends	[?]
Photos Tagged of You	Only Friends	[?]
	Edit Photo album privacy settings	
Videos Tagged of You	Only Friends	[?]
Friends	Only Friends	[?]
Wall Posts	<input checked="" type="checkbox"/> Friends may post to my Wall	[?]
	Only Friends	
Education Info	Only Friends	[?]
Work Info	Only Friends	[?]

Save Changes

Cancel

As a rule, it is best to use the most restrictive settings and then reduce security if you feel it is preventing you from doing something you would like to do.

In this example, I have set all my information to be viewable only by users whom I have agreed are my friends



The option '**Photos/Videos Tagged of you**' is important to understand. A friend may upload a photograph with you in it (and tag your name to that photo). If that person has a friend **who is not your friend**, they can still see it.

In this a further tab 'Contact Information'; from here there are additional settings that can be configured in the same way.

Search Menu

This page determines who can search for you and what they can see when they do search.

Facebook relies on users being able to find one another and requesting that they become friends. However, you must be careful what information can be seen when an anonymous user searches.

Privacy ▶ Search

Search discovery

Use the setting below to control who on Facebook can find you through the search function. Your Friends will always be able to find you.

Search Visibility

Search results

People who can find you in search can click through to a very limited version of your Profile. Use these tickboxes to control what people can see in addition to your name.

People who find me in a search can see:

- My Profile picture
- My friend list
- A link to add me as a friend
- A link to send me a message
- Pages I am a fan of

Public Search Listing

Use this setting to control whether your search result is available outside Facebook.

- Create a [public search listing](#) for me and submit it for search engine indexing ([see preview](#))

Please note that minors do not have public search listings - listings created by minors will activate only when they are no longer minors.

In this example, I have elected to allow every user of Facebook to search for me. However, if they do, they can only see a link to add me as a Friend. Once they send a Friend request, a choice can be made to either accept or deny that request based on personal preferences.



You may choose to allow a search to display your profile photograph, but if that is the case, you must be sure it is appropriate for all to see.

Case Studies

The following are several cases to consider when using Facebook.

Friend Requests

If you receive a friend request, try to wait until you see that person again before confirming their request.

Consider a recent example (*not at this school*) where a student created a profile under a teacher's name. The student sent friend requests to other members of staff and when they accepted that request, then used Facebook to gossip about and abuse other staff and students as well as having access to staff's personal information.

Friend Requests

Even if you only share information with friends, consider how appropriate that information may be before uploading it.

Consider this example. One of my friends has a brother at the school. She is friends with him, but I am not.

If she posts a photograph from a night out onto Facebook and tags me in that photograph. Her brother (as he is friends with her) can also see that photograph, the photo album and any subsequent comments made on that photograph.

Status Updates/ General Posting

Only post information onto Facebook that you would be happy for others to see.

If you fall out with another person (even if they are not on Facebook) you should not use Facebook as the forum from which to vent that anger. Regardless to the possibility that users may see the post, you must be aware of the slanderous nature of such posts.



***You are not above legal repercussions because you post online.
The Internet is not anonymous***

Consider the employee (again, not here) who rang in sick at work only to post a comment on Facebook about how he couldn't be bothered to go into work because he was too warm and comfy in bed. Another member of staff saw the post and he was subsequently dismissed.



***Nothing you do on the internet, no matter how secure you believe it to be,
is ever anonymous or private***

Befriending Students



Be aware that it is the schools position NOT to befriend students. It is also NOT advisable to add any photographs of students, however innocent. (even with parental permission).

It is possible that students may request you be friends on Facebook (especially when in sixth form) However, no matter how harmless and well intentioned this may be, this request must be refused.



If considering friend requests from former students, keep in mind that although a student may no longer attend school or college, their friends or relative may (refer to the advice in the **Safeguarding Protocols** booklet).

Conclusion

Facebook is a great tool for keeping in touch with friends and family if used correctly. However, if you are not aware of how information can propagate, it is far too easy for your personal information to be accessed by someone whom you would rather not access it.

As a general rule, you should:

- Use the highest privacy settings possible
- Only accept Friend request from users that you are sure are who they say they are
- Never upload any materials that may be inappropriate
- Remain professional at all times



Remember that nothing you do or say on the internet is completely anonymous or private

You should always conduct yourself online as you would offline.