E Safety Protocol

The purpose of this protocol is to offer guidance on safe use of the internet from a student perspective.

Profile

- This must be kept private in order to protect you from any potential threats
- When on social networking websites, you must be very careful as to what personal information you disclose.
- With most social media sites such as Twitter, Facebook, Instagram, Snapchat and many others, your information can be seen by anyone in the public unless you apply private settings in the privacy settings on those sites. It is important to make sure you do this when using any social media sites to protect yourself.
- It would not be advisable to display personal information such as:
  - Your address
  - Family details
  - Your own contact details.

  If you were to display these it could make you vulnerable, as people you don't trust with your information may be able to find it and use it.
- If you go into the settings on your Facebook page there will be a section entitled "privacy setting and tools." When selecting this you will be able to choose between three questions:
  - Who can see my stuff?
  - Who can contact me?
  - Who can look me up?

  By setting all of these to just 'friends' you will be fully protected as long as you only accept friend requests of people you know well.

Photographs

- They can be very revealing in terms of identifying you personally. Therefore if you upload any you must be very careful about what they reveal.
- With the privacy settings, as stated above, it is usually safe to upload photographs.
- It is extremely dangerous to send any form of explicit photograph to another member of a social networking website or via a text. The consequences of doing so can be very damaging. In no circumstances should an explicit image be sent to someone, even if you know them well.
- When uploading photographs, make sure you have the permissions of all the people in the photo as they might not want their image on the internet.
- Social media sites, such as 'Instagram' and 'Snapchat', are based on sending or showing photographs that you have. With these sites especially do not send photos to people you do not know. You can go onto your privacy settings on Instagram to make sure only people who are your friends can see your photos; this is key to making sure your pictures can't be seen by people you do not know.

Combating inappropriate behaviour

- If you are ever a target of any form of online abuse, whether it be cyber bullying or being messaged by someone you don't want to be, the first action to take is to block them. This will stop them being able to contact you. You should report their behaviour to your teachers, parents and, in extreme cases, the police, so it will be less likely to happen, not just to you, but to others as well.

- There are always people to talk to, such as your parents and your form tutor. By talking to them you will be able to discuss the issues you are having and then they will be able to advise you on how to deal with them. If necessary they will be able to solve the problems or inform others to help.

Friend/follow requests

- This is one of the most important parts of your internet safety.
- Even with the privacy settings set, as stated previously, you will not be safe unless you only accept friends and follow requests from people you know well.
- It is not a competition to see how many 'Facebook friends' you can obtain; the best thing to do is to only accept people you know you can trust with the personal information you have displayed in your profile.
- If you are not sure you know them well enough, do not accept them because you probably don't know them.

Are they who they say they are?

- A 'Catfish' is a person who pretends to be someone they are not and, by using social media, creates a false identity, normally with the intention of pursuing online relationships.
- It would not be right to say that you shouldn't talk to people on social networking sites as this is the main purpose of them, but you should only talk to people you know. However some signs of a catfish are:

    1. They don't have many friends on their Facebook profile and, in particular, when they upload photos with others in they have not tagged them. This suggests these photos are not their own.
    2. When you ask to talk via webcam or over the phone they will reject this and create excuses to as why they can't.

Messaging

- This applies to all social networking websites and messaging applications such WhatsApp, Kik, along with multiple others.
- It links in with many of the previous sections such as displaying photographs and posting statuses and it must be done with only friends.
- If someone messages you and you do not know them, even if you believe that they are trying to be friendly, you have no idea that they are who they say they are. Therefore, in situations like this, initially do not reply to the message and if they continue to attempt to contact you, block them. This can be done very easily on each website by either selecting their profile and blocking the person or by going into your own settings where there is the option to choose people you wish to block. This will stop them being able to message or see your profile and therefore protecting you from people you don't know.