Gaming, Online Friends and Privacy

How many different apps can you think of?

Write a list – they can be ones you use on your devices at home, or at school, or ones you know about. The images on the right might help.

Which apps do you think are free to download from the app store?

You might need to look on a device for this. Now identify those apps that require further purchasing to advance to the next level, or to make the app more effective, interesting or advert-free.

Just because an app is free to begin with doesn't mean it won't cost you! Often a game is easier to advance through if the player spends money. A credit card number isn't required because the device connects to the iTunes or Google Play store. Many free apps use in-app purchasing.

Of the apps that you have listed and those that you use regularly, for which ones is this statement true? Choose five apps and complete the grid below or draw it in your book:

App	Free?	Why you like this app

Don't forget that while sharing registration information is fine on a legitimate site or app and in fact part of what helps keep you safe, you should always ask an adult to help with this to ensure it is above board and ok to use. A website that is safe for posting secure information such as bank details or passwords will show or use the https and/or the 'padlock' symbol in the address bar.

Privacy Settings: You also need to look at privacy settings in order to keep yourself safe online. Each browser, social media site and app will have different privacy settings that may be accessed and changed in different ways and the settings will also have different significance depending on the information that app/site has access to. Everyone should always think about and check these settings, and if specific instructions are required it may be possible to search online for these.

However, some apps can (and do) ignore privacy settings, or may change them. Sharing personal information online within an app is different to registration information, as others can access it if they are on, for example, a gaming or social networking site. Therefore, you need to not only be careful about what you share but again to check your privacy settings, for example, 'public' and 'private' settings can control who can and cannot see your information.

Online Friends: Consider what might happen if your information and images can be accessed by:

- people you know but who are not yet categorised as a 'friend' on a site;
- friends on a site;
- people who are not friends on a site and that they don't know.

On gaming apps that you use, do you have any online gaming friends? These are probably mainly the friends you have in the real world. It is a great way to meet like-minded people and it can be fun to have lots of 'friends' on other 'networking' apps as well. However, how do you know that they are the people who they say they are?

Watch this video about the importance of privacy settings and staying cybersafe. After the clip, think about the importance of keeping your photographs and personal information private online.

TASK: Today, you will be adding another section to your quiz about 'Gaming, Online Friends and Privacy'. You have three challenges to complete.

Challenge One – Privacy: Watch the following video which is a warning from the Horrible Histories team about privacy settings and then complete the online activity on privacy (you will need Flash to play).

Challenge Two – Fake or Real Profiles: Can you spot which are legitimate and which are possibly fake friend requests? Use the prompt questions below:

- Do you know them in real life?
- Do they seem a bit 'too good to be true'?
- Can you see if they have other local friends who you know?
- Does their profile picture seem too professional or maybe you have seen it before?
- Are they asking for very personal information (where you live, your school name or full name)?

You have had 'friend' requests from the following people.

Jakeboy
You know Jake very well from school – he is in your class and you often hang out with him, both in school and at the park. You are expecting his friend request as you would like to share ideas and photos online.

Casey-Jane
You have never met Casey-Jane, but she seems very friendly and says that she is the same age as you and shares many of your interests. She mentions that she has seen you around and thinks she knows some of your school friends. She even suggests meeting up so that you know she is 'for real' and asks what your address is.

Mackers
You know Mackers is Chris Mackenzie from school – he knows some of your classmates. He has always been a bit unkind towards you at school, but maybe he wants to be friends after all. He has said that he is keen to share photos of a hobby that you have in common, which up to this point he has always teased you about.

CharlieG
You vaguely know Charlotte Gains. She goes to a different school, but you sometimes swim with her during inter school swimming galas. She has mentioned that she is changing schools and will be moving to your school soon and so wanted to be online friends. You have always liked her when you have spoken to her, although you don't really know much about her.

Challenge Three – Sharing information scenarios: When is it safe to disclose information and when is it not? Look at the scenarios below and decide what the consequences of each might be. What sort of information is ok to share and what is not?

1. You have just arrived on holiday and update your online status to say where you are and that you are having fun.

2. You want to buy a book as a gift so find a site online which has the padlock symbol. You check with your parents then enter bank card, name and address details.

3. You and a friend have headed off for the afternoon and are playing in a remote area. You take a selfie and post it online. Your privacy settings are set to public.

4. You have forgotten one of your passwords and request a reset online. An email arrives with a link to click on from the site you have just requested a new password from. You click on the link to reset the password.

5. You take some great photos on holiday and post them online on your return home.

6. You have clicked on a pop up advert as you want to buy the trainers it is advertising. The site seems legitimate, but doesn't have the padlock symbol or https in the url. You enter bank card, name and address details.

7. You receive an email explaining that your password needs changing and to click on the link to reset it. You click on the link and enter your old password, name and address.

8. You want to subscribe to National Geographic Kids magazine, but it needs personal information and you are not sure that you should be entering it online.

NOW COME UP WITH 1-2 QUESTIONS FOR EACH CHALLENGE TO ADD TO YOUR QUIZ

Sharing personal information

- Some home insurance companies will not pay out if you are burgled while away, if the fact you are away is disclosed publicly online in any way.

- You shouldn't click on any password reset links that you are not expecting – however, it is fine if you have just requested a reset.

- Putting bank card, name and address details online is fine if it is a secure site and you have permission to use a card from your parents or carers. Secure sites start with https, or may have a padlock symbol. You will also need to share this kind of personal information online if you have a bank account or you are subscribing or signing up for something like a magazine (with parental permission). These sites will also show that they are secure.