Viruses

*A **computer virus** is a program or piece of code that is loaded onto your **computer** without your knowledge and runs against your wishes.*

Ransomware
(Also known as Scareware) Infects your system and then makes you pay money to have it removed or threatens to damage all your files.

Worms
Usually try and find ways through your security, and then copy themselves and infect your system.

Trojans
Once on your system they record things like passwords and credit card details and send them to their owner.

Anti virus software scans you computer and if a virus is found it will remove it. However you must update it as new viruses are being made all the time.

Phishing

Phishing is the fraudulent practice of sending emails pretending to be from genuine company in order to persuade people to reveal personal information, such as passwords and credit card numbers, online.

Password Safety

Do:

- Choose a password with at least eight characters
- Choose a combination of upper and lower case letters, numbers and keyboard symbols such as @ # $ % ^ & * ( ) _ +

Don't:

- Choose your actual name or username.
- Choose family members' or pets' names.
- Choose your or family birthdays.
- Choose easy to work out background knowledge.
- The word 'password'.
- Numerical sequences.

UK Copyright Law

2 main purposes of the law:

1. To ensure *people are rewarded* for their creativity and hard work.
2. To *give protection* to the copyright holder if someone tries to steal their work.

In Computing, it protects people who create:

- Computer Software
- Music Downloads
- Website Images
- Web Page Text

Consequences for breaking the copyright law include: Fines and/or imprisonment.

Social Networking

CLICK CEOP Internet Safety

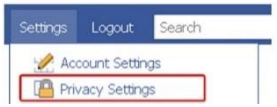
Social networking lets people share loads of information about who they are and what they like doing – with lots of different people.

However things can go wrong, these include:

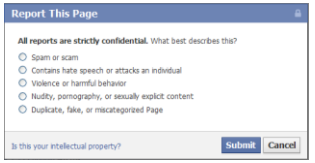
- **Sharing too much information** – the more information you put on line the more people can find out about you leading to things such as fraud or bullying.
- **Digital footprints** – Will you want things you post today to be hanging around in a few years time.
- **It's easy to lie online** – there are fake profiles online, people can pretend to be anyone which can have serious consequences.
- **Anti-social networking** – social networks can also be used to share nasty things e.g. embarrassing pictures, horrible comments etc.
- **I did NOT want to see that** – anyone can post videos, pictures or ideas on social networks that means you may see things you wish you hadn't.

To keep safe on social networks you can:

- Make sure that you know who your friends are.
- SHARE with CARE – would you be happy showing your parents or teachers the content you post?
- Use privacy settings.



- Know how to report e.g. Facebook report policy.



- Know how to get help e.g. CEOP.

CLICK CEOP Internet Safety

Cyberbullying

Cyberbullying is bullying that takes place using electronic technology.

Examples of cyberbullying include, mean text messages or emails, rumours sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

Cyberbullying can happen 24 hours a day even when a person is alone.

Cyberbullying messages can be posted anonymously and distributed quickly to a wide audience.

Deleting inappropriate messages is very difficult once posted.

If you are ever unsure, or in doubt then, speak immediately to a teacher, parent or carer!

Crofton Academy