

E-SAFETY HELPSHEET

SOCIAL NETWORK RISKS

- You never know who you're talking to
- Bullying
- Phishing - may lead to identity theft
- People being annoying or rude
- Grooming (Stranger Danger)
- Unsuitable use of photos



HOW TO STAY SAFE WHEN USING SOCIAL NETWORK SITES

The **DO's** of Social Networking

- Communicate only with people on your Contact List.
- Use a screen name that doesn't give away any sensitive information. .
- Check the terms, conditions and privacy statements of the chat site before you begin chatting.
- Use a chat nickname that doesn't give away any sensitive information.

The **DON'T's** of Social Networking

- Do not provide sensitive information (bank card number, passwords, address) about yourself in an IM conversation. Instant Messages are not encrypted, so they are easy targets for hackers.
- Do not agree to meet an unfamiliar person you came into contact with on IM. You can never know who that person really is.
- Do not download or accept files from people you don't know.
- Do not send your screen name online. People might find it and use it to send you unsolicited Instant Messages.
- Do not send private Instant Messages at school, your teachers may be entitled to view them.

REMEMBER STAY SMART - STAY SAFE

S	-	Safe
M	-	Meeting
A	-	Accepting
R	-	Reliable
T	-	Tell