

GUIDANCE FOR STUDENTS AND FAMILIES OF IES BRECKLAND

E-SAFETY

There are many steps you need to take to help ensure you are safe online, this includes everything from virus protection, checking your privacy settings and checking you have an up-to-date internet browser.

Recommendations

Anti-virus: Check you have anti-virus protection. Students and Parents remember there are many free antivirus packages. Make sure your anti-virus is up-to-date. If you are using a laptop offline remember to connect it to the Internet to update the anti-virus definition regularly.

Operating system: Always ensure that your operating system is up-to date. To turn on automatic updates in Windows XP do the following; Start > Control Panel > Security Centre > Turn on Auto Updates.

Internet Browser: A modern browser is integral to your safety online, features such as Phishing protection; help you to avoid giving out personal information to sites posing as a legitimate site.

Peer 2 Peer and Warez: These are notoriously dangerous and a high risk area for infecting you with viruses and spyware. Whilst they do offer many legal uses, P2P programs generally are used to share illegal files and often files posing as movies or music which are actually viruses.

Email: Many antivirus programs come with an included plug-in for scanning emails. Additionally online email providers such as Hotmail, Gmail and other web based email systems, such as ones provided by your ISP (internet service provider) offer online email attachment virus scanning. But it is always best practice to not open attachments in emails sent by an unknown address'.

SMART Rules

Safe: Keep safe by being careful not to give out personal information – such as your name, email, phone number, home address, or school name – to people who you don't trust online.

Meeting: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' knowledge.

Accepting: Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or offensive material!

Reliable: Someone online may be lying about who they are, and information you find on the internet may not be reliable.

Tell: If someone makes you feel uncomfortable or worried report it to a trusted adult. You can report online abuse to the police at: www.thinkyouknow.co.uk.

E-BULLYING

E-Bullying is particularly harmful as internet/electronic facilities are available 24hrs a day and can reach the victim in his/her home, where people generally feel safe.

Preventing

1. Always respect others
2. Think before you send
3. Keep your password secret

Responding

1. Block the bully
2. Don't retaliate or reply
3. Save the evidence
4. Tell a trusted adult. If the email bullying is occurring in school, then this should be dealt with through the school's anti bullying policy.

Online Protection

Whilst online it is important to ensure that your computer is protected from outside threats. This means having an active firewall and up to date antivirus software running in the background and set to run scheduled scans. You can still get caught out but making sure you have this in place helps reduce the possibility of infection.