What is F-TEC Open Minds?

Welcome to Open Minds. Open Minds is a bimonthly newsletter dedicated to the promotion and celebration of British values. Alongside this we will be keeping you up to date with any current and ongoing issues, we aim to keep you well informed whilst giving you an awareness of what is happening within the world. Our goal is to create an inclusive community where everyone feels valued and respected.

What are British Values?

Fundamental British Values underpin what it is to be a citizen in a modern and diverse Great Britain, valuing our community and celebrating the diversity of the UK. These values are:

Democracy - A culture built upon freedom and equality, where everyone is aware of their rights and responsibilities.

Rule of Law - The need for rules to make a happy, safe, and secure environment to live and work.

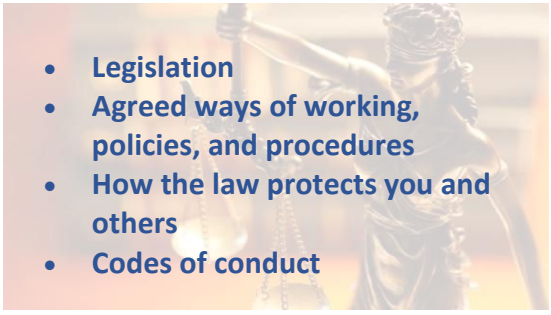
Respect and Tolerance - Understanding that we all don't share the same beliefs and values. Respecting the values, ideas and beliefs of others whilst not imposing our own on others. Below are some examples:

Individual Liberty - Protection of your rights and the rights of others you work with.

DEMOCRACY

- Leadership and accountability
- Joint decision making
- Team meetings
- The right to protest and petition.
- Receiving and giving feedback

RULE OF LAW



- Legislation
- Agreed ways of working, policies, and procedures
- How the law protects you and others
- Codes of conduct

RESPECT AND TOLERANCE

- Embracing diversity
- The importance of religion, traditions, cultural heritage, and preferences
- Stereotyping, labelling and prejudice.
- Tackling discrimination

INDIVIDUAL LIBERTY

- Equality and Human Rights
- Personal Development
- Respect and Dignity
- Rights, choice, consent, and individuality
- Values and principles

Online Safety

Online Safety is being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet. These could be security threats, protecting and managing your personal data, online reputation management, and avoiding harmful or illegal content.

Whether you call it E-Safety, Online Safety or Internet Safety, they all mean the same thing. Before 2015 the term used was E-Safety, but we know we mostly use the term Online Safety as this better represents the topic it refers to.

The number of people connected to the internet keeps growing daily, as does the need to recognise the challenges facing all of us using the online space.

By practicing Online Safety, we can prevent and minimise the risks that are involved with using digital technologies, platforms and services. Once the risks are managed, the internet can be enjoyed free from harm and to enormous benefit.

Online Safety in the UK Statistics

Online safety education helps everyone understand the potential risks and anything you may encounter online, such as cyberbullying, inappropriate content, and online predators, and empowers them to make smart choices to protect themselves and their peers.

The reality is that online grooming crimes have risen by 82% in six years.

Here's how the situation stood in 2024, according to research from the NSPCC:

- Since 2017, there have been around 34,000 online grooming offences in the UK.
- A total of 6,350 child grooming crimes were recorded in the year to March 2023.
- Children under 12 made up a quarter of the total victims.
- 80% of children aged 12 to 15 have had harmful experiences online.
- 150 different games, apps, and websites were used to target children.

Personal Online Safety

Here are some tips to tackle different areas of online safety.

Video Games

- Play age-appropriate games with content suitable for the maturity level.
- Set guidelines for screen time and encourage yourself to take regular breaks from gaming.
- Learn about the importance of online etiquette and respectful behaviour when playing multiplayer games.

Instagram

- Understand the importance of privacy settings and set profiles to private to limit exposure.
- Encourage open communication and talk to friends and family make sure they know that they can come to you if they encounter any issues or concerns.
- Think before you post and consider the potential consequences of sharing personal information or photos online - **Digital footprint does not go away!**

Snapchat

- Educate yourself about the risks associated with sharing disappearing messages and think carefully about who you add as friends on Snapchat.
- Never share your location or personal information with strangers on Snapchat.
- Report any inappropriate or concerning content you encounter on the platform.

Why Online Safety Education Matters

Online safety education plays a crucial role in keeping people safe in today's digital world.

By educating people about the potential risks, they may encounter online and empowering them to make smart choices, we can help ensure everyone stays safe and secure while enjoying the benefits of the internet.

Online Safety at the Workplace

With today's technology the importance of following the right tips for online safety in the workplace cannot be overlooked. As businesses increasingly rely on technology to conduct daily operations, you also become more vulnerable to cyber threats such as data breaches, phishing attacks, and malware infections.

Protecting sensitive information and ensuring the safety of employees is not just a technical issue. By implementing effective cyber safety measures, companies can safeguard their assets, maintain customer trust, and foster a secure work environment.

You go to work every day, often following the same routine, unaware of the online dangers and implications that we face. Keeping yourself and your organisation safe is part of your job and by becoming more aware of these dangers by making slight changes you can help keep yourself and your company safe from any cyber-attacks or breaches.

Top Tips for Online Safety at the Workplace

Here are some essential tips to enhance online safety at work and protect your organisation from potential threats.

1. Keep your password safe

- Do not share them with anyone.
- Do not leave them laying around.
- Change them regularly.
- Create strong passwords using a mixture of upper- and lower-case letters, numbers, and symbols.

2. Ensuring online safety at work - Authorised people only

- Do not let anyone tailgate you at your workplace entrance or at any other point throughout the building - It's ok to ask someone where they're going and if they don't seem familiar or don't have any identification.
- You should not expect anyone to let you into your workplace without your identification or confirming who you are.
- You should escort any unknown persons to a reception area to sign in. If you do not, you could potentially be allowing a fraudster access to your workplace where valuable information could easily be accessed.

3. Save everything on a shared drive/cloud

- Try to work from an online platform such as Microsoft SharePoint.
- Back up all your work regularly to a cloud service to avoid losing it in the unfortunate case of a ransomware attack.

4. Don't be tricked into clicking on links/attachments

- Always be cautious before you click on an attachment or link.
- With emails coming into your inbox every day, it's easy to be tricked into clicking on an attachment or link that looks like it was sent from someone you know.

5. Maintaining online safety at work - Update your computer

- Updates can sometimes seem inconvenient and it's very tempting to click the 'delay' or 'postpone' option, but updates can stop newly discovered security vulnerabilities by fixing gaps that could be used to attack your system.
- If you are running on older versions of your system and programs, you leave your computer open to these exploits.
- Anti-virus, anti-spyware and other security programs can keep your machine protected, but keeping your software up to date is one of the best ways of protecting against malicious code and hacking attacks.

6. Never give out account details

- You should never give your companies bank account details, payment information to anyone over the phone, email or online unless you know it is secure or from a person that you trust.
- If you are unsure, don't take any action until you can confirm the transaction with the appropriate person.

7. Avoid public wireless networks

- Public wireless networks may seem convenient, especially if you are travelling for work, but it can also be a threat to your privacy, meaning you might want to think twice about connecting.
- If you work for a company, you have a legal obligation to protect the privacy of your internet activity - Your home or workplace Wi-Fi is encrypted, but the coffee shop you may decide to do some work isn't - This means you're at risk of people monitoring your online activity.

- Wi-Fi uses radio waves, and radio waves are anything but direct. They broadcast, and this means that anyone within range can see everything you are doing online, if they have the right software.
- This means that, without protection, anyone who wants to can see - Every site you visit, every bit of text you send out and your login information for various sites.
- If you're connected to a Wi-Fi network, and have no idea whose network it is, beware - the hotspot might exist entirely to steal your personal data.
- Setting up a Wi-Fi network is neither hard nor expensive, and scammers have started doing so in the hopes they can steal passwords and other personal information. I
- If you connect to a network called something like 'Free Wi-Fi,' with no password required and no welcome screen, it might be a trap.

8. Keeping tidy and report anything suspicious to your IT support team

- If you have important files, passwords scribbled down and account details laying around, you are openly exposing confidential information for the world to see.

- Your details could be the gateway to exactly what a hacker needs to gain access to company information - This could have major consequences and a life changing effect on your organisation, so always keep a tidy workspace to avoid a breach.
- Whether it is an email attachment, an email from someone suspicious looking for information, or your computers performance being slow or unusual – always consult your IT support team.

Designated Safeguarding Lead –
Arizona Sykes
Emergency Mobile: 07425 783919
Office: 01793 384449
Arizona.Sykes@f-tec.org.uk

Deputy Designated Safeguarding Lead –
Wendy Cooke
Office: 01793 384449
Accounts@f-tec.org.uk

Segments from this article taken from:

https://swgfl.org.uk/online-safety/what-is-online-safety/#:~:text=Online%20Safety%20is%20being%20aware,avoiding%20harmful%20or%20illegal%20content

https://www.milk-education.co.uk/the-importance-of-online-safety-education/#:~:text=Online%20safety%20education%20helps%20children,protect%20themselves%20and%20their%20peers.&text=The%20reality%20is%20that%20online,by%2082%25%20in%20six%20years

https://www.metacompliance.com/blog/cyber-security-awareness/10-tips-for-cyber-safety-at-work#:~:text=Never%20give%20out%20account%20details,transaction%20with%20the%20appropriate%20person