Student Remote Learning

Top tips to stay safe and secure online

Due to COVID-19 situation there may be a time when you need to learn remotely. It does however require a level of discipline and careful planning. This guide aims to ensure that your experience is as safe and secure as it can be.

1. Treat remote learning the same as classroom learning

Despite being at home, it's important to remember the same rules apply as being in the classroom, particularly in terms of behaviour and conduct. Focus on learning and don't get distracted by your surroundings. To get the best experience from remote learning, it's important to create the right environment around you. Try to set up a mock 'classroom desk' at home in an open space, avoiding bedrooms as this could be inappropriate.

2. Use classroom language

If you are communicating through emails and online messages, don't use shorthand text speak and write as though you would speak in class. Remember to be respectful and polite and do not posting negative comments or spam the chat. Please report to your teacher / tutor / Head of Year if you are concerned about someone's conduct online. Always maintain classroom behaviour and remember that you are in a learning environment and not a social setting.

3. Take regular screen breaks

Spending prolonged periods of time in front of a screen isn't always healthy. Remember to take regular screen breaks where possible in your spare time, try to get some fresh air and enjoy other activities away from electronic devices.

4. Communicate through e-mail, or Teams and don't use college platforms to discuss personal matters

It's important that you send messages and any images required for class through approved college channels, such as Teams. This will help keep your personal information safe and secure. Keep college communication channels separate from personal communication channels. Don't be tempted to engage in casual discussions or send images, videos or links via official college platforms that aren't associated with your learning.

5. Don't share passwords or other sensitive information

In order to begin your online lessons or to gain access to learning materials, you have WSFC login details and passwords. In the same way you keep your personal details private, always keep these safe and never share them with others.

6. Look after your mental health and well being

Remote learning ultimately means working alone and missing out on daily social interaction with your friends. If you ever feel frustrated, low, or sad, it's important to discuss how you feel with your parents, friends, Tutor, or Head of Year to help keep your spirits up.

7. Stay safe online

E-safety is hugely important as we are spending more time online. If you have concerns around your safety or the safety of another member of the college community, please report to your tutor, Head of Year or another member of staff you feel comfortable with.

What is your digital footprint?

Whenever you visit a website, share a photo or make a comment online, you leave a digital footprint that other people can see. Your digital footprint includes all the information you share or that's collected about you online, and there can be a lot of it.

Lots of the information you share can be seen by other people. It can be used to target adverts at you, or it could be seen by a potential employer years later. Sometimes people can use the details you share to work out your identity.

Your footprint can be both good and bad. It could show things you're embarrassed about later or help people to see your skills or things you're proud of.

Tips to protect your privacy online

1. Change your privacy settings

Lots of social media sites will set your account to public by default. Changing your privacy settings lets you control who can see your posts and whether they'll appear on search engines.

2. Think before you post

You never know who'll see photos, videos or comments you put online so think about how others might react before you post anything. Even apps like Snapchat can be screenshotted and shared. Never share your address, phone number or the name of your College online.

3. Delete content you don't want online

Posted something you regret? There are lots of ways to delete things about you online. It can help to close or delete old social media accounts you don't use anymore as well.

4. Search your name

Typing your name or your username into a search engine can help you find what's easily available about you online. Remember, if you can find it then so can other people.

5. Check what data your device is collecting

Devices like phones, fitness trackers or wearables can collect data about you without you realising. Every device is different so search online to find out if your data is being used.

6. Set permissions for apps and websites

Lots of apps will ask for permission to use your data when you install them, including things like your contacts, photos and messages. Be careful about what you agree to and pick apps and browsers that protect your privacy. When you visit sites and you're asked whether you accept cookies, make sure you check what the website says about how they'll use them before you agree.

7. Share positive parts of your life

Try sharing things you'd be happy with anyone else seeing, things you are proud of. When you post comments to other people, be supportive and positive.

Useful links

www.thinkuknow.co.uk www.internetmatters.org www.childline.org.uk www.saferinternet.org.uk

Online learning - usage protocols for students

Below are excerpts from the Student Conduct policy and Acceptable Use policy which also apply to online learning:

Excerpts from Student Conduct policy

Section B

1. General Conduct

Refrain from acting in a manner which brings the College into disrepute or tarnishes the reputation of its staff or students.

Refrain from behaviour or expressing views that are contrary to fundamental British Values including democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs.

Treat all members of the College *(and online)* community with courtesy and respect at all times (including other students, staff and visitors). You are expected to follow instructions from any member of staff, and be truthful and fully co-operative in all dealings with the College.

Refrain from making personal comments about staff or students on social networks or other internet forums.

2. Academic

Refrain from noisy and/or disruptive behaviour. Behaviour which disrupts the learning of others will result in disciplinary proceedings. This applies to all areas of the College *(and online)* and its grounds.

Abide by the Acceptable Use Policy (see below)

Excerpts from WSFC Acceptable Use Policy For Students & Visitors

Introduction to the Acceptable Use Policy

All users (staff, students and visitors) of the computing facilities of the College are automatically bound by the terms of this Acceptable Use Policy (AUP).

General Use

You must not:

- create, store, transmit or knowingly receive any extremist material. (Extremism is defined as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance for those with different faiths and beliefs. It includes calls for the death of members of the British armed forces, whether in this country or overseas.)
- create, store, transmit or knowingly receive any fraudulent, offensive, defamatory, obscene, indecent or hurtful images, data or other material, or any data capable of being resolved into such material

continued on next page

- create, store, transmit or knowingly receive any material that is detrimental to the College's reputation, or that of its staff or students
- make personal comments about staff or students on internet forums, via email or internet sites including social networking sites
- use material in such a manner that applicable copyright laws are violated
- allow others to use their network account, or use someone else's network account with or without their permission
- be in possession of software that could be used to violate the privacy of other users (such software includes, but is not limited to, port scanners, password crackers, remote machine monitors and network traffic sniffers)
- undertake activities which:
    - use the facilities in any way that denies service or causes inconvenience to other users
    - attempt to bypass any security, anti-virus, monitoring or blocking features
    - make unreasonable demands of network resources

Accessing from home

All accesses to the College's IT facilities from outside the College are still bound by the terms of this AUP.

All reasonable effort must be made to ensure that College materials are not accessible to persons not connected with the College.

While every effort is made to ensure the integrity of available materials, the College offers no guarantee that files are free of viruses, and users should ensure that any downloaded item is checked on their local machine before use.

What will happen if you break the AUP

Breaking the Acceptable Use Policy will lead to disciplinary action which may result in suspension or exclusion. Please note that this will extend to activities unrelated to College where these bring the College into disrepute or suggest that staff, students, visitors or other members of the College would not be safe should the person concerned continue to be a member of the College.

A major violation of the AUP, such as extremism, accessing pornography or trying to break the network, will result in disciplinary action which may result in exclusion or suspension. Minor violations of the AUP will result in disciplinary action which may initially result in warnings, fines, the temporary loss of access to the IT network, and if repeated exclusion or suspension.

Any offence under English Criminal Law will be referred to the relevant police (or other) authorities.