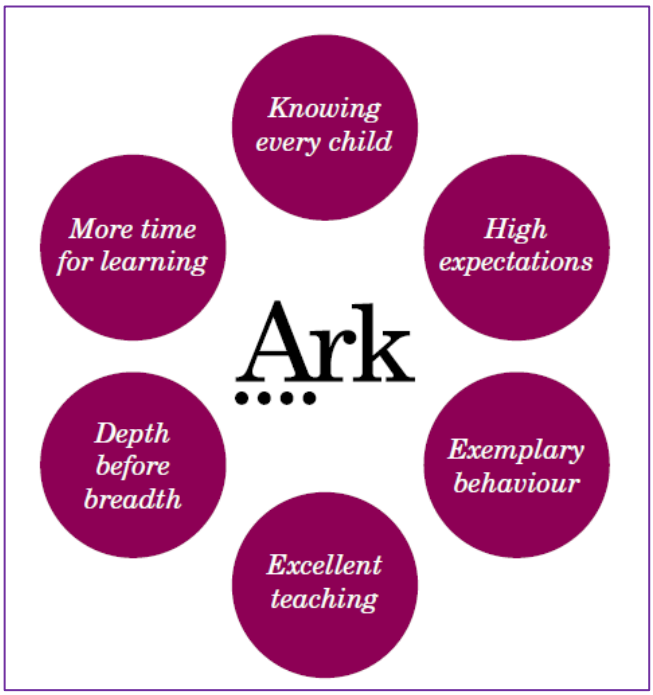
Ark Charter Academy

Ark Charter Academy's E-Safety Advice

Coronavirus (COVID-19) has seen our community day-to-day lives extremely disrupted. As a result, necessary actions have been implemented and our students are having to spend more and more time online been educated. This document has been drawn up to ensure the safety of Charters students, parents and the wider community remain safe while using the internet for educational and social purposes. It's vital that we ensure that our students should never experience abuse of any kind.



At Charter we foster an open environment in which our students, their parents and carers are encouraged to ask any questions and participate in ongoing conversation about the benefits and dangers of the online world.

Our students their parents and carers should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are always kept safe. Therefore, we at Charter recognise that:

1. We have a duty to ensure that all students are protected from potential harm online.
2. We have a responsibility to help keep students safe online, whether or not they are using Charter's network and devices.
3. Every student regardless of their disability, race, religion or belief, girl/boy or sexual orientation, have the right to equal protection from all types of harm or abuse.
4. We promote student's welfare and helping them to be responsible in their approach to online safety.

Staying Safe Online

It's not always easy to know what's safe online and what's not. The Internet is a fantastic source of fun and learning. However, it's worth following some simple rules to help keep you and your children stay safe online. At Charter we have come up with an exhaustive list of ways of keeping you safe, which have been sourced from trusted sites.

- You can adjust browser settings and filters to protect your children from unsuitable sites. To find out more on how to set up parental controls, go to https://www.internetmatters.org/parental-controls/ .
- If you have older children who want to explore on their own, it is a good idea to keep the computer in a family room or a place you share.
- Talk to your child about how to stay safe and let them know they can come to you if they find themselves in any sort of trouble. If you're not sure, please contact Team Charter.
- Think before you post. Don't upload or share anything you wouldn't want your parents, carers, teachers or family seeing. Once you post something, you lose control of it, especially if someone else screenshots or shares it.
- Don't share personal details. Keep things like your address, phone number, full name, school and date of birth private, and check what people can see in your privacy settings. Remember that people can use small clues like a school logo in a photo to find out a lot about you.
- Watch out for phishing and scams. Phishing is when someone tries to trick you into giving them information, like your password. Someone might also try to trick you by saying they can make you famous or that they're from a talent agency. Therefore, never click links from emails that ask you to log in or share your details.
    - If you're asked to log into a website, go to the app or site directly instead. **For example, only join MS teams from your teachers calendar invite not from the pop up.**
- Think about who you're talking to. There are lots of ways that people try to trick you into trusting them online. Even if you like and trust someone you've met online, never share personal information with them like your address, full name, school. **Remember**, follow the instructions above when using MS Teams
- Never give out your password. You should never give out your password or log-in information. Once someone has your password thy can potentially imitate you and do a considerable amount of damage to your image now and in the future. Especially when using MS Teams. If unsure, please get your password changed by contacting your tutor/teacher

- Cover your webcam. Some viruses will let someone access your webcam without you knowing, so make sure you cover your webcam whenever you're not using it. On most web cams the light will come on when in use, however since 2013 viruses have been created which are able to bypass the LED light. On how to secure your webcam go to: https://us.norton.com/internetsecurity-malware-webcam-hacking.html
- Use strong passwords to protect your devices and do not use the default password which comes with your new device (see the section on "Strong Passwords")
- Keep your apps and devices safe and up to date. Device and app updates include important security fixes, so it's good to make sure you regularly download updates or change settings to **automatic updates**.
- Make sure you log out when you're using public or shared devices. Lots of websites will keep you logged in, even after you close them. If someone else has access to the phone or device you're using, then they might be able to log into your account.
- Be careful which websites you're using. There are lots of websites that will try to trick you or pretend to be something else. You can be easily directed to another website which may appear authentic. Please remember, fake websites are designed to infiltrate your computer and cause damage. (see the section on "How to Spot a Fake or Scam Website")

Strong Passwords

A strong password will prevent someone from guessing your password. Malware such as viruses, spyware, trojans, worms and others use sophisticated algorithms to guess your password:

- Make your password more than 8 characters and use a mix of lower case letters, upper case letters, numbers and special characters (like %, #, ! and £).
- Don't use personal details such as favourite animal, your birthday or your best friend's name.
- Change your password regularly and use completely different passwords for different websites and apps.
- Don't use the default password or pin. Most default passwords/pins are 1234567 and can be broken in nanoseconds. If your unsure about the strength of your password, go to: https://www.my1login.com/resources/password-strength-test/ endorsed by https://www.ocr.org.uk/
- Set up 2-factor authentication. 2-factor authentication adds another layer of security to your password by asking for another piece of information

How to Spot a Fake or Scam Website

1. Pay attention to the address bar. Make sure any website you're using has "https" at the start of the address so that you know it's secure.

2. Only enter your log in details when you're absolutely sure it's the right website.
3. Check the domain name. A favourite trick of scammers is to create websites with addresses that mimic those of large brands or companies, like Yah00.com or Amaz0n.net.
4. Watch for poor grammar and spelling. An excess of spelling, punctuation, capitalisation, and grammar mistakes could indicate that a website is fake. Remember, it's all about image. Poor SpaG (spelling and grammar) portrays a poor image.
5. Look for reliable contact information. There will be ways to contact the company (phone, email, live chat, physical address) and try them out
6. Run a virus scan. A flood of ads or pop-ups can indicate that a site isn't secure. Ads themselves aren't an indication of a problem, but if there are more ads than content or if you have to click through several ads to be redirected to the website, you have cause to be suspicious. If your device/broadband is running slower than usual, then it can be an indication that your device has bean infected by malware (worm or trojan).

Other sources of information

Bullying and cyberbullying - If you or someone you know is being bullied
Sexting and sending nudes - If you've been sexting and something's gone wrong.
Online gaming - learn how to stay safe online when playing games.
Online grooming - what you need to know to keep you and others safe.
Mobile phone safety - Tips to keep you safe when using your mobile or smartphone.
Report a nude image online – when nude image or video have been shared online
Being bullied because you're deaf - Being bullied is never your fault.
Online porn - It's natural to feel curious about porn. help answer all your questions.