

## **E-safety Guidance for Students**

The following information has been produced to provide information about taking practical steps to stay safe when using technology.

It contains the names of recognised organisations that provide interactive information and support in each section.

### **Chatting**

#### **What is chatting?**

There are lots of different ways you can chat to people online - and lots of different places you can do it. Chatting includes every type of service which allows you to have a conversation with somebody else. It can be text based messaging (such as instant messaging or SMS) or via a voice or video link (such as by VoIP internet phone calls or a webcam). It can also be instant, real-time communication (chat rooms or instant messaging) or delayed (such as e-mail or voicemail). Chatting like this is a great way to stay in touch - as well as meet new people. But there are a few things you can do to make sure you have a good time and stay safe.

#### **Things to think about**

- Know who you're talking to online; if you don't know someone face to face they could be anyone
- Remember – what you do or show on your webcam can be recorded and what they do or show on their webcam at the other end might be a recording
- Avoid having one-sided webcam conversations where the other person's webcam is 'broken' or, 'not working...'; you won't know who they really are, what they are doing or who they are watching with

#### **Things to do**

- Keep your personal information private - avoid sharing personal information such as your phone number, home address or photographs with people you don't know in person and trust
- Check whether the service you use allows you to create friend lists. These lists let you manage who sees what. For example, you may only want your closest friends to see some information
- Keep your clothes on when using webcam - images of you could end up in the wrong hands
- Use private messages for people you know in person and trust; be careful of private messaging people you don't know
- Use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you've ever shared it in the past, change it)
- Know how to block someone if they make you feel uncomfortable or upset
- Learn how to save chat logs and texts so that if someone does make you uncomfortable/upset, you have the evidence to report them

- Remember to log out of a service properly after use, especially on a shared computer

### **Additional advice for parents/carers**

- Talk to your child about who they're talking to online and encourage them to think before talking to people they don't know in person
- Try to understand and guide your child's online behaviour - negotiate and establish boundaries and discuss sensitively the issues around the concept of 'friends'
- Familiarise yourself with the chat programme your child uses. Find out more about its built-in safety functions and how they can be contacted within the service
- Ask your child if they know how to block someone who they don't want to talk to anymore. If they don't, help them to learn how to use the blocking feature
- Use parental control software provided by your internet service provider, mobile phone network, online content provider or games console and consider using filtering options, monitoring and setting time limits for access to chat
- If you discover misconduct between your child and someone online stay calm, investigate the facts and seek expert help if needed
- As part of a wider discussion about sex and relationships cover how people may use the internet to explore their sexuality, which may include sexual chatting

### **Reporting**

- If someone makes you feel uncomfortable, talk to an adult you trust, such as a relative or teacher. If you would prefer to talk to someone in confidence you can contact Childline (0800 1111). If someone has acted inappropriately online towards you, or someone you know, you can report directly to the Child Exploitation and Online Protection Centre (CEOP). It could be sexual chat, being asked to do something that makes you feel uncomfortable or someone asking to meet up.
- If someone is bullying you, there is help and support available from Bullying UK. You can also contact the College's designated protection officers for advice and support.
- If the problem concerns issues of privacy, or a breach of terms of service, report the incident to your Personal Tutor, Head of Studies or Student Services team.

### **Sharing**

#### **What is sharing?**

If you have something you're proud of then it can feel good to share it with others. Maybe it's a photo you've taken or a video you've made. Maybe you have opinions and thoughts you want to share on a forum or in your own blog, or you want to share your interests with people who like the same things as you. One of the great things about sharing on the internet is that it's so quick and easy - you just click a button on your computer, smartphone or digital camera and it's there online. But that can also be the problem. If you post something in haste you may regret it later and by that time it may be

too late to get it back. Here are some things you should think about before you ever share anything online.

### **Things to think about**

- Once you've shared something online you've lost control and ownership of it. Depending on the content of what you share this could mean the College will need to take action under other policies and rules, for instance Safeguarding, disciplinary or even contacting the police.
- Remember that people may still be able to see things you share online months or even years into the future
- If you're unsure about what you should and shouldn't share online, ask yourself this: 'Would I show this to my parents/carers/teacher?' If you wouldn't, then don't share it online
- Some people could use information or things you've shared in ways you don't like or couldn't have imagined
- Some people could share things about you which are upsetting - without your knowledge

### **Things to do**

- Find out how to use the privacy settings on the services and devices you use. These settings will help you take control of your information so that you can decide what information you will share, and who you will share it with
- Keep your personal information private – this includes photos of you and your friends, your school's name, email, phone number, date of birth, address and location; only share them with people you know and trust
- Only upload pictures of yourself which you would be happy for your parents/carers or teachers to see
- Only share details of your location with people you know in person and trust

### **Additional advice for parents/carers**

- Set up a family email address you can all use to fill in online forms
- Set clear guidelines for your children about what is ok to share about themselves and about your family – lead by example and explain what you have shared and why; be aware that comments posted by your children could impact on you and your family's reputation
- Talk to your children about how easy it is for people to assume another identity online
- There are a number of ways that you can set your own lists of sites you want to block access to; activating your internet service provider's parental controls, or those of another provider, can make this easy for you
- Install reputable internet security software on your computers and mobile devices; keep this and operating systems up to date
- Be aware that children can access the internet through publicly available wifi for example in shops, coffee bars and bus termini; check whether your children's devices have built in wifi connectivity and see if there are any tools to help manage access to inappropriate content

- As part of a wider discussion about sex and relationships cover how people may use the internet to explore their sexuality which may include sharing sexual images
- Be aware that smartphones often contain location technology. This technology finds the mobile's position and provides services related to where you are. Talk to your child about who they share this information with

## Reporting

- Know/learn what to do if you have shared something you shouldn't have – *[point out how users can report to you on your service here]*
- If someone has shared information about you which upsets you, or if someone is making you feel uncomfortable, talk to an adult you trust, such as a relative or teacher. If you would prefer to talk to someone in confidence you can contact Childline (0800 1111). If someone has acted inappropriately online towards you, or someone you know, you can report directly to the Child Exploitation and Online Protection Centre (CEOP). It could be sexual chat, being asked to do something that makes you feel uncomfortable or someone asking to meet up.
- If someone is bullying you using your information, there is help and support available from Bullying UK
- Know what to do if something online has upset you: talk to Childline or the Samaritans if you are feeling desperate or sad and go to Report-It to report incidents of race hate. You can also report to us if our terms of service have been broken speak to your Personal Tutor, a Student Liaison Officer or Head of Studies.

## Gaming

### What is gaming?

Playing games online against other people can be really enjoyable and great fun. You can do it via a mobile phone, a computer or a games console and online games come in every shape and form. There are the ones where you each take a turn - like chess on a mobile phone app - and others where you compete to get your scores as high as you can on a leaderboard. Then there are the 3D virtual worlds where hundreds or thousands of people are simultaneously playing against each other. Online gaming has something for everyone and millions of children and young people across the UK regularly take part. Below are some tips to ensure you get the most out of your online gaming experience.

### Things to think about

- When you're gaming as part of a network this often involves live online chat and you're playing with real people
- You should be respectful to others in the game and understand the rules and boundaries of the website or community

### Things to do

- Keep gaming friends 'in the game' – avoid sharing personal information with people you've met in games and avoid giving them your social networking profile

details or email address. Also, choose a user name that does not reveal any personal information about you

- Use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you've ever shared your password in the past, change it)
- Learn how to block people you don't want to be in contact with any more. If you experience any bullying, hacking and racism, save the evidence and report it
- Remember to always log out of a service properly after use, especially on a shared computer
- Experts recommend you take regular 5 minute breaks every 45 minutes to an hour to help your concentration

### **Additional advice for parents/carers**

- Young people can also go online through some gaming devices and online gaming often involves playing against real people
- Use the PEGI games ratings to guide you when buying games for your child or making judgements about the games they are playing. The PEGI system rates video games at various age levels (3, 7, 12, 16 and 18) and is designed to protect children and young teenagers from inappropriate content
- Make sure your children are using games from reputable and legal online providers
- Online gaming can be compulsive for some; be aware of the amount of time spent online and set boundaries around your child's use
- Games should be played as part of a healthy and balanced lifestyle; regular 5 minute breaks should therefore be taken every 45 minutes to an hour
- Use parental controls on games consoles to disable or restrict access to facilities such as voice chat. They can also be used to disable online credit payments or applications that you feel are inappropriate
- You can use online parental controls to restrict or block access to online gaming websites and other content altogether
- Familiarise yourself with the chat programme your child uses. Find out more about its built-in safety functions and how they can be contacted within the service
- Install reputable internet security software on your computers and mobile devices; keep this and operating systems up to date

### **Reporting**

- Know where to get help if someone is bullying you in a game – report it to your service provider or Bullying UK who can provide help and support
- If someone is upsetting you or making you feel uncomfortable, talk to an adult you trust, such as a relative, tutor or College designated protection officer. If you would prefer to talk to someone in confidence you can contact Childline (0800 1111). If someone has acted inappropriately online towards you, or someone you know, you can report directly to the Child Exploitation and Online Protection Centre (CEOP). It could be sexual chat, being asked to do something that makes you feel uncomfortable or someone asking to meet up.

## **Content providing (including downloading)**

### **What is content providing?**

There is so much information available on the internet that it's like having the world's biggest library at your fingertips. But not everything you read and see online will be true, and not everyone will be who they say they are. It is also illegal to download some files, while others could be infected with viruses which steal your personal details and pass them on to thieves. Below are a few things you need to consider when browsing the web - and a few steps you can take to keep yourself safe.

### **Things to think about**

- Not everything you read or see online is true - it is easy for people to make things up or alter photos on the internet
- There are things online you might find upsetting and distressing – you will know what these things are
- Downloading may harm your computer or mobile device and could be illegal - just because you can download something, it doesn't mean that you are allowed to or should do, as copyright law applies online. This is especially true of illegal file-sharing sites
- If you make music, film or TV available to others on a file-sharing network, download from an illegal site or sell copies without the permission of those who own the copyright then you are breaking the law; use legal sites that reward the creators for their work
- Copying someone else's ideas and passing them off as your own is called plagiarism – the College has rules about this, see the College handbook or speak to a tutor for further advice and information.

### **Things to do**

- Learn how to block pop ups
- Check whether information is true by looking on at least two other sites; ignore sites you don't recognise and consider carefully what you are reading
- Use reputable sources of information such as organisations or brands you know and trust
- Only download files from websites you are sure are safe to use; sites might contain malicious software (such as viruses) which could damage your computer or steal your personal information.
- Only open attachments or click on links in emails you are expecting; if you get a suspicious-looking email, even from a friend, it might not be genuine if their computer has been infected by a virus and you should not open it
- Think – if an offer seems too good to be true, it probably is

### **Additional advice for parents/carers**

- Set safe search filters and lock this on for a particular desktop computer, laptop or mobile
- Use parental controls to manage access; mobile operators use network filters which block over 18 content; these are free of charge and are mostly set as 'on' by default for all contract and prepay customers



- Use software filters on computers, laptops and mobiles; most fixed internet service providers offer these free to customers
- Around one in every 100/200 emails can contain malware (a piece of malicious software which takes over a person's computer) or phishing attacks (attempts to access your personal details, such as usernames and passwords): install reputable antivirus or firewall software on your computer or mobile and make sure you keep this and operating systems up to date
- As part of a wider discussion about sex and relationships, cover how people may use the internet to explore their sexuality, which may include viewing pornography
- Ask your child's school to share their plagiarism rules with you

### **Reporting**

- If you come across something which upsets you, tell us as service provider. Talk to an adult you trust, such as a relative, teacher or designated protection officer. If you would prefer to talk to someone in confidence you can contact Childline (0800 1111). You can talk to Childline or the Samaritans if you feel sad or desperate, B-eat for eating disorder support and Report-it to report incidents of race hate. You can also report to us if our terms of service have been broken
- Illegal child sex abuse images online can be reported to the Internet Watch Foundation (IWF) or your local police
- You can report fraud or online scams or viruses to Action Fraud – the UK's national fraud reporting centre
- Get Safe Online provides advice on how people can use the internet confidently, safely and securely

### **Networking (closely relates to 'sharing')**

#### **What is networking?**

Online communities - such as social networking sites - are some of the most popular sites on the web. Millions of people log onto these sites every day to hang out with their friends and talk about their lives. When you sign up you get the chance to create and customise your own profile and you can upload your favourite photos and videos. There are even networks within networks where you can join others who share the same interests, or who live in the same area or go to your school. Most people will have a great time being a member of these sites - but it's important you take care, particularly when giving out information about yourself. Here are some tips on how to network safely.

#### **Things to think about**

- Adding someone as a 'friend' means they (and sometimes their friends) may be able to see the things you share, share things with you and even share things about you; can you trust them with your information?
- It's easy to lie online, not everyone is who they say they are

#### **Things to do**

- Learn about privacy settings to take control of your information and decide what information you will share, and who you will share it with - use lists/groups to share different information with different 'friends'

- Avoid friending people you don't know in person and sharing personal information with them such as your phone number, home address or photographs
- Learn how to block 'friends' in case you feel you need to, and keep the evidence
- Use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you've ever shared it in the past, change it)
- Think very carefully about meeting someone face to face who you only know online; if you do decide to do this, never go without taking a trusted adult with you
- Only upload or share pictures of yourself which you would be happy for your parents/carers or teachers to see
- Remember to properly log out of a site after use, especially on a shared computer

### **Additional advice for parents and carers**

- Keep an open dialogue with your child about who they're talking to online and why they should think before talking to people they don't know in person; try to understand and guide their online behaviour just as you would for their offline activity; negotiate and establish boundaries and discuss sensitively the issues around the concept of 'friends' (and 'friends of friends')
- Use parental controls to restrict or block access to social networking sites; device-level parental controls mean you can set up unique settings per user so that you can restrict access to particular networks based on the user
- Explain why it's important to be honest about your age online, for example in signing up to social networking sites – advertising and other content will be aimed at the age the user says they are
- As part of a wider discussion about sex and relationships cover how people may use the internet to explore their sexuality

### **Reporting**

- If someone is making you feel uncomfortable, talk to an adult you trust, such as a relative, teacher or College designated protection officer. If you would prefer to talk to someone in confidence you can contact Childline (0800 1111). If someone has acted inappropriately online towards you, or someone you know you can report directly to the Child Exploitation and Online Protection Centre (CEOP). It could be sexual chat, being asked to do something that makes you feel uncomfortable or someone asking to meet up.
- If someone is bullying you using your information, there is help and support available from Bullying UK.
- Know what to do if something online has upset you: talk to Childline or the Samaritans if you are feeling desperate or sad, B-eat for eating disorder advice and Report-it to report incidents of race hate. You can also report to us if our terms of service have been broken by speaking to your Personal Tutor, a Student Liaison Officer or Head of Studies or College Designated Protection Officer



## Shopping and commerce

### What is commerce?

Online shopping brings the High Street to your fingertips, wherever you are. The internet offers great choice and shopping online can be really convenient - there are no closing times, or queues, and you can compare deals from dozens of online stores to get the best deals. There are also other forms of shopping that are unique to the internet. For example, you can pay for virtual goods and services such as virtual currency to spend in games on social networking sites. But while online shopping can bring many benefits, there are also some risks. Below are a few things you need to look out for when shopping online - and a few steps you can take to ensure you're not left out of pocket.

### Things to think about

- Remember – if an offer seems too good to be true, it probably is
- It's also a good idea to look for unbiased reviews of online retailers. Cross-check information on the internet and see if anyone else has had problems
- Beware of online scams, which can be very convincing; check that online stores have a physical address and telephone contact details

### Things to do

- Buy from reputable retailers online – brands and services you know well in person, or which you have researched thoroughly
- When paying for goods and services online, make sure the website address in the browser window begins with https:// – the 's' stands for 'secure' and ensures that any personal and financial data cannot be intercepted during transactions
- Look for the padlock symbol on payment pages. Don't be fooled by a padlock that appears on the web page itself. It's easy to copy the image of a padlock. You need to look for one that is in the window frame of the browser itself
- Always use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you've ever shared your password in the past, change it)
- Never follow links to shopping or banking sites – always type the address straight into the address bar
- Tell the truth about your age and do not lie about it to obtain goods or services which are age restricted – if you do you will be breaking the law
- Remember to always log out of a service properly after use, especially on a shared computer

### Additional advice for parents/carers

- Ensure that you and your children check for the padlock symbol in the window frame of the browser *[similar to the example shown above]*: only 25% of 12-15s do this when visiting new sites according to Ofcom
- Talk to your children about safe online shopping and supervise purchases with younger children – explain that criminals can set up online shops that are only there to steal money, so check out the website carefully, be careful when disclosing any personal/financial/payment information and ensure that the site is using a secure payment method

- Check bank and card transactions regularly for unrecognised transactions
- Install reputable internet security software on your computers and mobile devices; keep this and operating systems up to date – security software provided by your internet service provider or third party can tell you whether a site is secure or not

### **Reporting**

- If the problem concerns issues of privacy or is a breach of our terms of service, report the issue to us broken speak to your Personal Tutor, a Student Liaison Officer or Head of Studies.
- You can report fraud or online scams or viruses to Action Fraud –the UK's national fraud reporting centre
- Get Safe Online provides advice on how people can use the internet confidently, safely and securely