PEOPLE SERVICES
DN COLLEGES GROUP

E-Safety Handbook for Students

DN COLLEGES GROUP

Doncaster College

UNIVERSITY CAMPUS DONCASTER

North Lindsey College

ucnl University Campus North Lincolnshire

Humber Energy Skills Training Academy

Contents

Introduction

In today's digital world, we're constantly using the internet, social media, apps, and online games. While these tools make life fun and more connected, it's important to stay safe and make smart choices. This guide is here to help you understand how to protect yourself from online dangers, avoid risky behaviour, and use technology in a positive way.

DNCG Core Values

ASPIRE

Ambition:
To achieve the highest standards.

Support:
A caring, safe, and inclusive environment.

Partnership:
Collaborative working to achieve shared goals.

Innovation:
We use our initiative and are agile in finding creative solutions.

Responsibility:
We take individual and collective responsibility.

Equality:
We work with integrity and are open, honest, and respectful of each other.

Who's Here to Help with E-Safety?

Designated Safeguarding Lead (DSL) and Deputy DSLs (DDSLs)

These staff members are responsible for keeping you safe both online and offline. They get special training in E-Safety and are the ones who decide how to handle online safety issues.

Safeguarding Team

Safeguarding Team is trained to deal with online safety problems. They keep an eye on internet activity at the College, investigate any E-Safety concerns, and make sure everything is properly recorded.

Personal Development Team

This team teaches E-Safety through special sessions during the year. They make sure E-Safety is part of your personal development lessons.

IT Infrastructure Team and Business Systems & Information Team

These teams to protect the College's digital systems. They monitor the network to make sure it's being used safely and block any harmful websites when necessary.

Academic Services Team

This team creates E-Safety resources, like presentations and training materials, that help both you and staff stay informed about E-Safety.

DNCG DSL's

Rachel Maguire
Executive Lead for Safeguarding

Sally Macdonald
Designated Teacher for Children in Care and Designated Safeguarding Lead

What is E-Safety?

E-Safety is all about protecting yourself online and knowing how to handle digital risks. Whether you're using social media, playing online games, or browsing websites, it's important to be aware of potential problems like cyberbullying, inappropriate content, or people trying to trick or scam

The key areas of E-Safety include:

- **Content:** What you see online – Is it appropriate? Could it harm you?
- **Contact:** Who you talk to online – Are they trustworthy? Could they be harmful?
- **Conduct:** How you behave online – Are your actions safe and responsible?
- **Commerce:** Are you being tricked into spending money or giving out personal information?

Understanding Online Risks

There are different types of risks online and understanding them can help you avoid difficult or dangerous situations. Being aware of how to respond to these risks is key to staying safe.

Cyberbullying

Cyberbullying is when someone bullies or harasses you online. This could happen through messages, posts, or spreading harmful rumours. If you experience cyberbullying, don't respond or engage with the person. Instead, block them and report the issue to a trusted adult or a safeguarding team. Keep screenshots or records of any messages as evidence.

Inappropriate Content

Sometimes, you may accidentally come across material that isn't suitable for your age, like violent, hateful, or sexual content. Avoid clicking on suspicious links or pop-ups and be mindful of what's shared in online groups. Many platforms allow you to report inappropriate content. Use the reporting tools available and talk to an adult if you're unsure.

Grooming

Grooming is when someone builds a fake relationship with you online to gain your trust and manipulate you. This person may pretend to be a friend or act like they care, but their goal is to extract personal information or arrange a face-to-face meeting. Always be cautious when interacting with people you don't know in real life. Don't share personal information (like your address, college, or pictures) and report any suspicious behaviour to an adult or the platform.

Sexting

Sexting refers to the sharing of intimate images or messages. Once these images are sent, they can be copied, shared, or used to humiliate or blackmail you. Remember, it's illegal to send or possess indecent images of someone under the age of 18, even if you are under 18 yourself. Think carefully before sharing anything and never feel pressured to send something you're uncomfortable with.

Online Scams

Online scams involve tricking people into giving away personal details, passwords, or money. Scammers may use phishing emails,

fake websites, or direct messages pretending to be someone you know or trust. Be cautious of emails or messages that ask for personal information, promise rewards that seem too good to be true, or threaten you. Use strong, unique passwords, enable two-factor authentication, and never share your passwords.

Fake News and Misinformation
Not everything you read or see online is true. Fake news and misinformation can spread quickly through social media and websites. Always verify the source of information, check multiple reliable sources, and think critically before sharing or acting on information.

AI Generated Content & Deepfakes
Technology is now able to create very realistic photos, videos, and audio using Artificial Intelligence (AI). These can look real even when they are completely fake. This includes deepfakes, which are videos or images that make it appear as if someone said or did something they never did.

- Deepfakes can be used to spread lies or embarrass people. If something looks strange or feels too shocking to be true, check other sources before believing or sharing it.
- Never share or create images or videos of others that look edited, inappropriate, or suspicious. They may be fake, harmful, or illegal.
- If you think you've seen a deepfake of yourself or someone else, report it to a trusted adult or the Safeguarding Team immediately.

Privacy and Data Protection
Personal data can be collected without your knowledge when you're online. Be mindful of the websites and apps you use and review their privacy settings. Only share what's necessary, and avoid sharing private information like your home address, phone number, or financial details.

AI Tools and Your Data
Some apps use AI to analyse your photos, voice, or personal information. Always check the privacy settings before using these tools. Avoid uploading personal images or sharing private details unless you fully trust the platform.

Addiction to Technology
Spending too much time online can lead to unhealthy habits, such as neglecting college work or social relationships. Set limits on your screen time and take breaks to engage in offline activities.

Radicalisation
Radicalisation occurs when someone is encouraged to adopt extreme views, often leading to support for violent behaviour. Extremist groups may use social media to spread their ideas and recruit vulnerable individuals, often targeting those who feel isolated. If you notice changes in someone's behaviour—like sharing hateful views or joining extreme online groups—avoid engaging and report it to an adult, the safeguarding team, or authorities like **Prevent** in the UK.

Staying Safe Online: Tips and Best Practices

Here are some key ways to keep yourself safe while enjoying the benefits of being online:

Protect Your Personal Information
Don't share details like your address, phone number, or college online. Keep your passwords private and strong, using a mix of letters, numbers, and symbols.

Set Up Strong Privacy Settings
Use the privacy settings on your social media accounts to control who can see your posts and personal information. Regularly review your settings to make sure they're up to date..

Think Before You Post
Anything you post online can be copied or shared, even if you delete it later. Think carefully about the photos, videos, or comments you share. Ask yourself if you'd be comfortable with your family, teachers, or future employers seeing it.

Be Respectful
Just as you should behave kindly in real life, the same rules apply online. Don't post things that might hurt or offend others. Avoid engaging in negative online behaviour like trolling or bullying.

Report and Block
If you encounter someone harassing you, sharing inappropriate content, or behaving suspiciously, report them to the platform and block them immediately. You can also talk to an

adult or your Safeguarding Team at College for help.

Your Digital Footprint: Why It Matters

Your digital footprint is the record of everything you do online. This includes what you post on social media, the websites you visit, and even the comments you make. Future employers, colleges, or even friends might look at your online activity, so it's important to keep it positive and professional.

Types of Digital Footprints:

- **Active Footprint:** This is the stuff you actively share, like photos or comments.
- **Passive Footprint:** This is data collected about you, such as the websites you visit or location data from apps.

Tips for Managing Your Digital Footprint:

- **Search Yourself Online:** See what information comes up about you when you search your name.
- **Keep It Clean:** Delete old posts or photos that no longer reflect who you are or that you wouldn't want others to see.
- **Use Separate Accounts:** It's smart to have a professional account (like LinkedIn) for college or work, and a private one for personal use.

How to Handle Cyberbullying

Cyberbullying can happen in many forms, such as hurtful messages, rumours, or even threats shared online. Here's what to do if it happens to you:

- **Don't Respond:** It can be tempting to reply, but responding can escalate the situation.
- **Save the Evidence:** Keep screenshots of the messages or posts in case you need to report the situation later.
- **Block and Report:** Block the person who is bullying you and report them to the platform.
- **Talk to Someone:** Speak to a trusted adult, whether it's a parent, teacher, or someone from the Safeguarding Team at your college.

Skills Boost & Online Resources

These E-Safety courses will introduce you to the essentials of staying safe online, including how to protect personal information and demonstrate respect in online interactions.

Skills Boost

Online Training – Getting Started with E-Safety

Student Skills Boost training for the getting started with E-Safety

Getting Started with E-Safety is available in Year 1 of Skills Boost

Online Training – Being Safe Online

Student Skills Boost training for the recap on online safety

Being Safe Online is available in Year 1 of Skills Boost

Teams and Blended Learning Guidance

Microsoft Teams is used for online lessons, meetings, and communication at college. To get the most out of online learning, it's important to follow good E Safety practice.

- Join lessons in a quiet, suitable space.
- Only use your college account when accessing online lessons.
- Follow your tutor's instructions about camera and microphone use. This includes using background blur and muting your mic when not in use.
- Be respectful and behave as you would in a classroom.
- Only share files or messages appropriate for a learning environment.
- Report anything concerning to your tutor or the Safeguarding Team.

Blended Learning Consortium – E-Safety Resources

These E-Safety courses will introduce you to the essentials of staying safe online, including how to protect personal information, recognise cyberbullying & online grooming and digital wellbeing.

Online Training – Getting Started with E-Safety

Blended Learning Consortium online courses for students

Ask your tutor for help accessing this E-Safety resource

Videos

These videos will guide you through essential tips for protecting your privacy, managing your digital footprint, and staying safe online.

Video – Online Safety and Privacy
This series will guide you through the essentials of E-Safety, helping you protect your personal information and make informed decisions in your digital life.

Online Safety and Privacy - ClickView

Video - Digital Footprints and You
This programme covers managing your digital identity, the risks of sharing information, sexting dangers, and social media safety, with tips on reducing your footprint and presenting your best self-online.

Staying Safe Online: Digital Footprints and You - ClickView

Inspiring Digital Enterprise Award - iDEA

The Inspiring Digital Enterprise Award, known as iDEA, is an international award-winning programme that helps you demonstrate digital, enterprise and employability skills for free..

E-Safety
The E-Safety & Online Etiquette badge is part of the iDEA Bronze Award and is in the Citizen category, helping you learn digital awareness, safety and ethics.

E-Safety & Online Etiquette | iDEA

Safe Online
The Safe Online badge is part of the iDEA Bronze Award and is in the Citizen category, helping you learn digital awareness, safety and ethics

Safe Online | iDEA

Social Media Ethics
The Social Media Ethics badge is part of the iDEA Bronze Award and is in the Citizen category, helping you learn digital awareness, safety and ethics.

Social Media Ethics | iDEA

Cyber Security
The Cyber Security badge is part of the iDEA Bronze Award and is in the Citizen category, helping you learn digital awareness, safety and ethics.

Cyber Security | iDEA

Social Media Platform Guidance

Use privacy settings across social media platforms to manage your digital footprint. The following guidance is provided by each of the major social media platforms. Click to read detailed information.

- Facebook - Basic privacy settings and tools
- X (formerly Twitter) - How to protect and unprotect your Tweets
- YouTube - Privacy and safety
- Instagram - Privacy settings and information
- LinkedIn - Account and privacy settings overview
- Snapchat - Privacy settings
- TikTok - Privacy and security settings

Daily Monitoring

All users of our Wifi and / or a DNCG laptop or PC will be subject to our filtering and monitoring systems that safeguards our students. We use a product called Smoothwall. Smoothwall is 'always on' 24/7.

Users will have their internet and computer use monitored and inappropriate use will generate an alert is there is a safeguarding concern. The Safeguarding Team receive alerts for concerning online behaviour and will take appropriate action to address this with staff and students. Further information about Smoothwall can be found here.

Websites

To help staff, students, and parents stay informed and safe online, we've compiled a list of valuable E-Safety websites. These resources offer expert advice, practical tips, and tools to navigate the digital world securely. From understanding online risks to managing digital footprints and safeguarding against cyberbullying, these sites provide comprehensive support for creating a safer online environment. Explore these links to find guidance tailored to your needs and stay ahead in the ever-evolving digital landscape.

CEOP – www.ceop.police.uk/safety-centre
A service to report online abuse or exploitation and access advice for staying safe online.

ThinkUKnow – www.thinkuknow.co.uk
A resource for advice on staying safe online, tailored for different age groups, parents, and professionals.

NSPCC Online Safety – www.nspcc.org.uk/keeping-children-safe/online-safety
Offers tips and advice on how to keep children safe online, including social media and gaming.

Internet Safety Day – www.saferinternetday.org
Dedicated to promoting safer and more responsible use of online technology and mobile phones, featuring educational resources and events.

Internet Matters – www.internetmatters.org
Provides guides for parents and educators on how to help children navigate online risks and stay safe.

Childnet – www.childnet.com
Focuses on helping children, parents, and educators understand online safety and digital wellbeing.

Get Safe Online – www.getsafeonline.org
Offers free expert advice on all aspects of online safety for individuals and families.

UK Safer Internet Centre – www.saferinternet.org.uk
Provides resources, tips, and tools for safe internet use across all age groups.

Stay Safe Online – www.staysafeonline.org
Provides tips and resources for protecting yourself and your family from online threats.

Common Sense Media – www.commonsensemedia.org

E-Safety Concerns

All students of the College community are encouraged to report any E-safety concerns they may have. This includes concerns about cyberbullying, inappropriate content, online harassment, and any other online safety issues. Reports can be made through the following channels:

- **Safeguarding:** Concerns can be reported directly to the team, who are responsible for handling safeguarding issues, including E-safety. Students are also encouraged to speak to their tutor.
- **Anonymous Reporting:** Students can also report bullying, harassment and victimisation using the push button service on the College website.