Online Safety Policy

1. Introduction

As an online institution, technology is fundamental to DATA LAW learners. You have access to technology for the purposes of learning through DATA LAW platforms (such as the VLE or webinars), and you might also access non-DATA LAW platforms for the purpose of learning (for instance online research, or the formation of student social media groups). It is the responsibility of DATA LAW to safeguard its learners online. This guidance document establishes how DATA LAW approaches your online safety, and how you may keep safe online.

2. Definitions

Term	Definition
Cyberbullying	Bullying which takes place involving the use of technology (for a definition of bullying, please see the Bullying Procedure).
Sexting	The sharing of sexual imagery (including videos), or sending of sexually explicit messages, using technology.
Grooming	Where an adult forms a relationship with a child (or vulnerable adult) for the purpose of sexual abuse, exploitation or trafficking.
Hate Speech	Communications where hatred is expressed towards a person or group of people due to a protected characteristic (for example, protected characteristics such as race, disability, gender).
Radicalisation	The process someone undergoes whereby they come to support a terrorist group or ideology.

3. Guidance

3.1 Online Safety Do’s and Don’ts

3.1.1 Do’s:

To stay safe when using technology, and to avoid getting into difficulties please:

- Keep usernames and passwords safe and secure. Do not share usernames or passwords, and don’t write down or store passwords where they might be stolen or accessed by another person.
- Consider when it is appropriate to share personal information about yourself online, and do not share information about others online.
- Report any unpleasant or inappropriate materials or messages seen online, including in personal social media groups of DATA LAW learners, to the Designated Safeguarding Lead.
- Respect others’ work and property by not accessing, copying, removing or otherwise altering any other user’s files, without the owner’s knowledge and permission.

- Be polite and responsible when communicating with others, do not use strong, aggressive or inappropriate language and appreciate that others may have different opinions.
- Do not take or distribute images of anyone without their permission
- Do not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- Do not try to download copies (including music and videos) where work is protected by copyright
- Take care to check that the information accessed is accurate when using the internet to find information.
- Ensure that you comply with all of the terms and conditions of the DATA LAW platforms that you use.

3.1.2 Don'ts

To remain safe online, it is important to avoid unacceptable use of technology. Some usage is both illegal **and** unacceptable, and these have been highlighted separately below for your guidance:

Illegal and unacceptable:

- Child sexual abuse images
- Grooming, incitement, arrangement or facilitation of sexual acts against children
- Possession of extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character)
- Criminally racist material in UK- to stir up religious hatred (or hatred on the grounds of sexual orientation)
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Promotion of extremism or terrorism
- Infringing copyright

Unacceptable:

- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of violence or mental harm
- Any other information which may be offensive to colleagues or breaches the ethos of DATA LAW or brings DATA LAW into disrepute
- Using DATA LAW systems to run a private business not associated with DATA LAW
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by DATA LAW
- Creating or propagating computer viruses or other harmful files

3.2 Cyberbullying

Cyberbullying is a form of bullying which involves the use of technology. It can take many different forms and could involve behaviours such as abusive messaging, intimidation, spreading of rumours or imitating the victim online. DATA LAW regards bullying, in all forms, as unacceptable, and its approach to bullying is set out in its Bullying Procedure.

Victims of cyberbullying may wish to:

- Report the bullying to the owners of the platform where it has occurred
- Where possible, 'block' the bully on the platform where they are contacting the victim
- Report the bullying to DATA LAW for investigation, or ask DATA LAW for advice or support, by emailing the Designated Safeguarding Lead.
- Report the bullying to another party for support (e.g. a family member, or GP)

3.3 Sexting

This guidance has been separated into two sections, due to differences in the law for those who are under the age of 18. Anyone who wishes to receive further advice or guidance on the below can request this by emailing Designated Safeguarding Lead.

Learners aged under 18	**All Learners**
It is **illegal** to create, possess or share sexual images or videos of a child. This includes situations where a child shares sexual images or videos of themselves (for example where they are in a relationship). When an adult forms a relationship with and sends sexual messages to a child, this is known as 'grooming'. Grooming is **illegal**. Please see section 3.5 for more information. Anyone can report known or suspected illegal conduct relation to online child abuse to the Police or CEOP. If you view child abuse images or videos by accident, you should stop viewing these as soon as possible.	Consenting adults may choose to share sexual images or videos as part of a healthy relationship. It is advised that once an image or video is shared online, the poster no longer has control of how this content is used or shared. It is possible that content may be used for the purposes of bullying, blackmail or causing harm to another person. Where someone shares sexual images or videos that they have received from another person without consent, this is known as **revenge pornography**. This practice is **illegal**.

3.4 Online Pornography

The internet is a common and easy way to search for pornography. People search for pornography for many reasons- they may be actively looking for it, or it may even appear in a pop-up or be stumbled upon by accident. There are some tips for staying safe when looking at pornography online:

- Some young people use pornography as a way to learn about sex. It's important to remember that pornography isn't real, and the sex in pornography is very different to the way that many people look and have sex in the real world. Do not use pornography to base what a healthy, consenting sexual relationship looks like.
- Be sure that you are clear on consent. If you try something that you have seen in porn, have you discussed this with your partner, and do they consent (remember, consent should be explicit, not implicit)? Have the people appearing in the pornography given their consent- if not, this is illegal and you can get into trouble for watching/sharing it.
- Be aware that watching porn can be addictive. Try to limit the amount that you watch, and ask for help if you feel you have become addicted. You can do so by emailing the Designated Safeguarding Lead.
- Don't feel pressured to watch pornography if you don't want to. Not everyone watches porn, and this is okay.

3.5 Grooming

In the context of this guidance document, DATA LAW refers to the grooming process which takes place online and where the product of this process is a sexual relationship between an adult and a child (or vulnerable adult) which may take place in person or online. The product of this process is known as Child Sexual Exploitation.

The grooming process may involve a perpetrator (who may pretend to be a young person) befriending a vulnerable young person online. They may develop a relationship with the young person, making them feel listened to or flattered. The young person may be tricked or forced into sending images, text or videos to their abuser online. Abusers may then blackmail or coerce their victims into sending further material, perhaps by threatening to share the material online or with friends and family of the victim.

To protect yourself from grooming, you might:

- Only accept friend requests online from people that yourself or a friend has met before in person
- Try to confirm the identity of who you talk to online- consider whether they have multiple accounts, and whether you can search for the person on the internet
- Scrutinise the things you are told by strangers, and consider whether they make sense or might be untrue
- Do not meet up with someone you have met online. If you do so, make sure it is in public and that you take a friend.
- Report any contact you are uncomfortable with or unsure of to CEOP, the Police, or discuss this with the Designated Safeguarding Lead.

3.6 Hate Speech

In the UK we have freedom of speech, however there are some restrictions placed upon this by law. For example, we cannot spread hatred against an individual or a group due to a protected characteristic or make threats of violence.

Some guidance surrounding avoiding hate speech includes:

- Considering carefully how you put your opinion across. For example, you can disagree with a certain religion and its principles, but you cannot spread hatred about this religion or make threats towards them.
- Engage with other learners professionally and respectfully.
- Be wary of 'trolls', who may say inflammatory things to get a reaction.
- Be clear on how to block people, or to remove content/conversations which make you feel uncomfortable.
- If you are unsure of whether something is appropriate to discuss, mention it first to your coach or the Designated Safeguarding Lead.

3.7 Radicalisation

Radicalisation may occur through several different means, supported by the use of the internet. For example, people may actively search for extremist content, or may stumble across this by accident. They may also be 'recruited' online by a radicaliser.

The internet is a common platform whereby radicalisers recruit people to their cause. The process for radicalisation can be very similar to the process of grooming described above. The extremist selects a vulnerable victim, and may form a friendship. The victim may become gradually isolated from their friends and family, and gradually exposed to more and more extreme content and ideas. The eventual aim may be for the victim to commit and extremist act, or to help recruit further people to the cause. DATA LAW has a comprehensive Code of Practice and Policy in relation to Prevent, and this advice relates to how learners can keep themselves safe online in this area:

- Assess the credibility of websites that you visit. Consider whether they are reputable sites, and whether there are other reputable sites which back up what they are saying.
- If you talk to strangers online, be wary of what they say and/or ask you to do. Never meet up with someone you have met online- and if you do, ensure that this is in a public place and that you take a friend with you.
- Consider the information that you share about yourself online. Radicalisers often look for vulnerable individuals to target, so if you have shared these vulnerabilities online you may be more likely to be contacted.
- Be confident to report sites, content or people that makes you uncomfortable.
- Contact the Designated Safeguarding Lead if you are unsure about any of the above, or wish to discuss this further.

3.8 Social Media

3.8.1 Managing your accounts

Social media is a popular way to communicate with others, and DATA LAW acknowledges that many of its learners will use social media accounts. To stay safe when using social media, DATA LAW advises that learners know:

- Who can view their content (both their personal information, and what they post)
- Who can contact them
- How to block someone
- How to stop seeing something which makes them uncomfortable

3.8.2 Social media and your employer

Learners might wish to consider how they appear to others on social media. Many prospective (and current) employers check social media accounts, and posting the wrong content can, and has, stopped people from gaining employment. Some things to think about include:

- Ensuring that any profile pictures or statuses are appropriate- try to avoid pictures where you are drinking alcohol, look inebriated or are doing anything which may be considered 'unprofessional'.
- Don't post any comments about employers on social media- you can be fired for doing so. People often use social media as a place to 'vent' but this is not appropriate in relation to your employment.
- Don't post on social media during working hours (unless this is your job)- it's advertising to your employer that you are doing something other than working.
- Make your profile private- this way people cannot see what you post, if you do choose to do any of the above.

3.9 Online Communities

3.9.1 General tips

Wherever you engage with other people online, you become part of the 'online community' for that platform. Many social media sites have their own community standards, and you are expected to comply with these rules to be allowed to continue to use that site/app. Some general tips for engaging in an online community include:

- Remember that once you have posted something online, it's out there forever- even if you delete it, others might have copies. Don't post anything you might regret.
- Consider whether you are sure what you are posting is true- and how you know this.

- Get involved in debates, but watch out for internet trolls (people who intentionally goes out of their way to annoy/intimidate others online for their own amusement)- it can be easy to get drawn into arguments with these people and can be very frustrating,
- Be polite and respectful- disagree with people, but don't be rude about it.
- Remember, if it's illegal in real life, it's illegal online too- just as things such as harassment are illegal to do in person, you also cannot harass people online.

3.9.2 Tips when using the VLE

The VLE is a good tool available to learners, that allows them to interact with other learners- through the use of the forums, or by messaging others. It's important to remember that the VLE is primarily designed for education, and so it's not always appropriate to engage with this platform in the same way you would with other platforms (for example with social media). Some tips regarding this include:

- Think of your fellow learners as your colleagues- if you wouldn't be allowed to say something to your colleague, you also probably shouldn't say it to another student.
- Try to consider other people intentions. It can be easy to misconstrue what people mean when they type things, as you can't hear tone of voice or see facial expressions. If something upsets you, try and think about whether it was meant in a different way.
- If someone gets something wrong, try and explain this to them in a kind way. Everyone is here to learn, and part of that is making mistakes. Be polite in how you tell them about these.
- Report anything you are unhappy with to your tutor, or to the Designated Safeguarding Lead.

3.10 Digital Crimes

3.10.1 Hacking and Viruses

Internet criminals use many tactics to cause damage to individuals. They may wish to hack into your computer to gain information (such as your personal details or banking information), or they may even wish to just destroy your machine to make in unusable.

To help keep yourself safe from hackers and viruses, you can follow these tips:

- Have strong, secure passwords- include a mixture of random words, and try to include numbers, capital letters and special characters. Use different passwords for each of your accounts.
- Download antivirus software onto your machine.
- Be aware of what scams look like (see section 3.10.2).
- Try to only visit reputable websites that you have heard before.

- Don't download something if you don't know what it is, or who has sent it.

3.10.2 Scams

Sadly, there are lots of scams online. The aim of many scams is to gather money or personal information from vulnerable individuals. Scams can take many forms:

- Emails from what look like 'reputable' companies (for instance banks or companies that you shop with), saying you owe money or that you need to give them up to date bank details or passwords etc.
- Emails from companies telling you that you have 'won' or been offered something- a prize, a lottery… if you didn't enter/apply for any of these, it's likely that it's a scam.
- Job offers, where you are told that you can make quick money. Scammers will often come up with attractive rouses, informing you that you can make quick money for little work- and that you will need to give them your bank details so that you can be paid.
- Online romances- criminals form an online, romantic relationship, and then ask for money (usually under the pretence that they need money for something such as airplane tickets).
- Fake news- news stories which are made up. They often look like they are real news stories.

To help protect yourself from online scams, you should:

- Not click on links within emails.
- Check email addresses- does the email address look legitimate? If not, it could be a scam.
- Never send personal information about yourself via email. If they require personal information, you should visit the company's legitimate website (not one that they provide a link to within the email) and call the customer services to discuss this. You should **never** give your password to anyone, even on the phone.
- Do not open attachments from unknown senders, or emails which look suspicious.
- Never send money to someone you have met romantically online unless you have met them face-to-face. If you refuse to send money, and they become very forceful or aggressive, this can be a further sign of a scam.
- Check what you read online, and always question whether the site looks legitimate-does the logo look right, are there spelling mistakes, do the dates add up