# Trust me

# Teachers guidance

**Thinking critically** about what you see online

## Introduction

The internet provides a fantastic platform for young people to share their ideas, talents and passions with a huge online community of people from all over the world. However, this means that young people need to become ever more critical about the information they see online. In light of extremism, grooming, inaccurate information and online scams, the purpose of this resource is for students to learn how to think critically about the content they see and the people they interact with online. Through discussion and mocked-up examples, this resource aims to give students the skills to question inaccurate information online and to explore the motives behind the content we see and the people we speak to. The secondary pack will also explore the idea of propaganda and consider how this may be presented online.

This teacher guidance provides you with the appropriate background documents for schools and additional content to help you to deliver this resource to pupils. It will give you an overview of the relevant laws online and case study examples to support you in answering any questions during the sessions.

## Content


1. The laws online
2. FAQs about online behaviour regarding critical thinking
   - Questions from students
   - Questions from teachers
3. Case studies about online trust
4. Further links to advice


## 1. The laws online

### Identity theft

Identity theft laws make it illegal to adopt or exploit another person's identity. These laws encompass fraud, obtaining other people's personal information for the purposes of financial gain, scams and impersonation. The relevant laws are:

- **Theft Act 1968:** This act explains that stealing someone's identity is similar to stealing someone's property. It mentions manipulating information for the purposes of stealing goods and false accounting.
  http://www.legislation.gov.uk/ukpga/1968/60
- **Data Protection 1998**: This Act explains that a person's private information (race, age, sex, sexual orientation, health records, and financial records) can't be divulged. It outlines that UK citizens have the right to obtain information about themselves and it also lays out how long companies can hold on to personal information of people on databases.
  http://www.legislation.gov.uk/ukpga/1998/29/contents
- **Identity Cards 2006:** This Act covers passports and identity cards and seeks to protect against personal identity theft. This act also legitimises the collection of personal information without consent for crime and justice purposes.
  http://www.legislation.gov.uk/ukpga/2006/15/contents




By Childnet – CC – BY –NC – SA 4.0

- **Fraud Act 2006:** covers “phishing” and “hacking” or misrepresenting your identity. ‘Phishing’ refers to the fraudulent practice of sending out falsified emails from ‘reputable’ companies in the hope that people will reveal their passwords and personal information. http://www.legislation.gov.uk/ukpga/2006/35/section/2

**More information to be found here:**

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275784/13-521-identity-related-crime-uk.pdf

**Counter- terrorism and security**

There are laws that exist that protect the UK from threats to national security. These laws fall under the Security Service Act 1989 and the Counter Terrorism and Security Act 2015. The role of MI5 is “*the protection of national security and in particular its protection against threats such as terrorism, espionage and sabotage, the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.”*

The counter terrorism act reveals that internet data can be searched in the interests of national security.

http://www.legislation.gov.uk/ukpga/2015/6/section/21/enacted

**Grooming**

Grooming refers to the practice of an adult contacting a child online or offline, with the intent of meeting and potentially harming that child. More recently we have seen this also include an adult making contact with a child to obtain explicit pictures in order to exploit that child. Grooming comes under the updated Sexual Offences Act 2003 whereby intent is also a factor in the sentencing of the perpetrator. Online cases of grooming should be reported to CEOP, the Child Exploitation and Online Protection Unit, who are a branch of the National Crime Agency. https://ceop.police.uk/

http://www.cps.gov.uk/legal/s_to_u/sentencing_manual/s15_grooming/

**Hate crime**

The Crown Prosecution Service (CPS) define a Hate Incident as any incident which the victim, or anyone else, thinks is based on someone’s prejudice towards them because of their race, religion, sexual orientation, disability or because they are transgender. Not all hate incidents will amount to criminal offences, but those that do, become hate crimes. Some hateful online messages regarding race, religion etc. may be perceived as hate speech and can be reported at True Vision - http://www.report-it.org.uk/

http://www.cps.gov.uk/northeast/victims_and_witnesses/hate_crime/

**Malicious communications**

The Communications Act 2003 section 127, see Stones 8.30110B, covers the sending of improper messages. Section 127(1) (a) relates to a message that is grossly offensive or of an indecent, obscene or menacing character and should be used for indecent phone calls and emails. Section 127(2) targets false messages and persistent misuse intended to cause annoyance, inconvenience or needless anxiety.

**Malicious communications including threats of violence**

The Malicious Communications Act 1988 section 1, see Stones 8.20830, deals with the sending to another of any article which is indecent or grossly offensive, or which conveys a threat, or which is false, provided there is an intent to cause distress or anxiety to the recipient. The offence covers letters, writing of all descriptions, electronic communications, photographs and other images in a material form, tape recordings, films and video recordings. Poison-pen letters are usually covered.



By Childnet – CC – BY –NC – SA 4.0

Particularly serious examples may justify a more serious charge, e.g. threats to kill.

The offence is one of sending, delivering or transmitting, so there is no requirement for the article to reach the intended recipient.

http://www.cps.gov.uk/legal/a_to_c/communications_offences/

## 2. FAQs about online behaviour regarding critical thinking

### Questions from students

**There are lots of scams and so much misleading information online – should we believe anything on the internet?**

Online content has not been put up by computers but is instead a reflection of the people who put it there. We know that in the offline world there are people who seek to scam us or mislead us and the online world is no different. Being a critical thinker doesn't mean rejecting all information online, it merely means not accepting information immediately at face value, instead you should think critically about the information that is in front of you, weighing up what you know to be true and what is written and checking with others if you are unclear. Sometimes you may make mistakes and it is easy to fall for scams as they can be very realistic. Always remember if things seem too good to be true then they usually are and check a few different websites instead of relying solely on the first site that comes up on a search engine. Remember, you can always look in a book, and check with other people as well! There is always a reason for posting content online and it is important to think about what this reason/motive could be, and then to make an informed decision.

**How are you meant to know if someone you're speaking to online has a hidden agenda, if they don't say anything worrying?**

Just like in real life, people can be misleading. Someone who you thought was your friend, can betray you, or deceive you. Online, it can be trickier to gauge a person's moral character as you are not speaking face-to-face. It is also quite easy to pretend to be someone you are not online. You will not be able to pick up on the small mannerisms or facial expressions that might give away the fact that someone is lying to you. However, this is not to say that everyone who speaks to you online is lying to you. Many people connect online and make genuine relationships. However, it is important, to be wary of people who you only know online. If you have never met them before, they are still a stranger and even if you have a picture of them, it can be difficult to guarantee that it is actually them. Remember, if anyone makes you uncomfortable online, asks you lots of personal questions, challenges you to do something you wouldn't normally do or tries to isolate you from your family and friends, be wary of this and report to CEOP (https://ceop.police.uk/) or to the counter terrorism unit (www.gov.uk/report-terrorism).

**Some people are more adventurous than others – should we never take risks online? What if you had entered a competition, you don't want to miss out!**

True, there are genuine competitions that exist online and if you won, it would be a shame not to collect your prize. However, be wary of information online that 'guarantees immediate results' or anything that sounds too good to be true. Be careful about giving away personal information or clicking on links sent by strangers, as this might be a phishing exercise. Phishing is defined as the attempt by seemingly trustworthy organisations to acquire personal information, such as passwords and bank details, from people so this information can be used for malicious purposes.


By Childnet – CC – BY –NC – SA 4.0

**Can you say what you want online? Where is the line between freedom of expression and propaganda/hate speech?**

Freedom of expression is incredibly important and the internet is a fantastic platform for people to share their views with the world. However, human rights also come with responsibilities and it is important to be aware of how our actions may impede on others. You have the right to show support for a cause you believe in, but you do not have the right to incite or promote violence against others. Social media sites, in particular, don't allow people to express support for violent, criminal or racist behaviour that could be perceived as hate speech. Your account may be restricted or blocked if you do decide to engage in this type of behaviour.
You can find more information about what social networking sites will allow in the links below:
**Facebook:** https://www.facebook.com/communitystandards
**Instagram**: https://help.instagram.com/477434105621119/
**Snapchat:** https://support.snapchat.com/en-US/a/guidelines
**Twitter:** https://support.twitter.com/articles/18311

**What happens if you report inappropriate content online?**

You can report hate crimes to True Vision who are a branch of the police (http://www.report-it.org.uk/your_police_force). On most social media sites, should you see anything such as spam, violent or inappropriate content, you have the ability to report such posts or videos. The more context given at the time of the report, the better the reporting system will be, and reading the community guidelines or terms and conditions of the site should give a good indication of what kind of content breaks the Terms and conditions of a certain website. Should someone make a report, the reported content will be taken to one side and reviewed by a member of the safety team at that particular organisation. If the post goes against the rules of the site, the offending post will be removed and they may take action against the account responsible, ranging from a warning to banning that person from the site. It is important to bear in mind that not all reported content breaks the rules of the platform. Although you may find the content or opinions of others distasteful or offensive, everyone is entitled to an opinion and if it doesn't break the rules of the platform, this content may not be removed.

## Questions from teachers

**What if my students don't see the risks or harm in the same way as adults?**

Young people may lead you to believe that 'they know everything' about being safe online, or they might over-estimate their ability to help themselves out of a situation. Often, they claim that that it 'wouldn't happen to me' or they struggle to see any negative consequences that might occur. As a teacher, it is important to listen to students and hear their reactions, but also to challenge them if necessary, introducing case studies as a way to show them how vulnerable young people can be online. See section 3 of this document for case studies you could use and explain that especially in the cases of grooming and extremism, young people may not be aware of the process as it happening to them. The purpose of this resource is to encourage young people to think critically about what they see and who they speak to online, and part of this is to be aware of the worst case scenarios, should they arise.

**What should I do if I'm worried one of my students is being influenced by someone online?**

If you have noticed a change in a student's behaviour, or if you someone lets you know that they are worried about a friend who is speaking to someone online, these are safeguarding issues and should be treated as such. Grooming and radicalisation are serious matters and a report should be made to the Safeguarding Lead in school.


By Childnet – CC – BY –NC – SA 4.0

## 3. Case Studies about online trust

### Cautionary tales (scams/things to watch out for online)

### SMiShing (SMS phishing):

The victim receives a text message that they are about to be charged for a service they never ordered. They are told that they need to contact the company immediately to cancel the order or be responsible for the charge. The text includes a hyper-link, which the victim clicks on, taking them to a fake website that triggers the download of a program that breaches the security features of their phone.

### Phishing:

The victim receives an email from their bank telling them that they need to update their password immediately or risk having their online banking service shut down. The victim clicks on the link in the email, which takes them to a fake ("spoofed") bank site where they are instructed to enter their username and current password. They comply and in so doing, gives the fraud operator their on-line banking login information.

For more information and examples, go to the Fraud Avengers site - **http://fraudavengers.org/scams/**

More information about up-to-date scams can be found at Action Fraud, the national fraud and cyber crime reporting centre - **http://www.actionfraud.police.uk/**

### Online grooming case studies

Breck Bednar, 14, was murdered after he was befriended by Dayne Lewis on an online gaming network.

http://www.theguardian.com/lifeandstyle/2016/jan/23/breck-bednar-murder-online-grooming-gaming-lorin-lafave

Ronan Hughes, 17, took his own life after being blackmailed by a foreign, criminal gang when he sent a sexually explicit photo of himself to someone he thought was a girl online.

http://www.mirror.co.uk/news/uk-news/ronan-hughes-teenager-was-being-5854921

Adam Johnson, Sunderland footballer, was jailed for 6 years after being accused of grooming a 15 year old girl by initially connecting with her on Whatsapp.

http://www.theguardian.com/uk-news/2016/mar/24/adam-johnson-should-be-jailed-for-up-to-10-years-court-told

### Radicalisation and extremism case studies

Guardian article outlining how four young Britons were drawn to jihad.

http://www.theguardian.com/uk-news/2016/mar/31/brighton-to-battlefield-how-four-young-britons-drawn-to-jihad-syria

Guardian article questioning why young Britons are travelling to Syria

http://www.theguardian.com/commentisfree/2014/jun/24/isis-british-muslims-reality-war-fight-extremism

FATE is a charity that stands for Families Against Terrorism and Extremism and contains stories from families who have suffered when their child left to fight with extremists. It outlines the reasons why they believe their son or daughter got involved in this type of behaviour and also the impact it has had on them as a family.

http://www.cbc.ca/player/play/2685025644/
http://www.findfate.org/



By Childnet – CC – BY –NC – SA 4.0

## 4. Further links to advice

### Other relevant documents for schools

Department for Education: Advice about promoting fundamental British Values

- Guidance for maintained schools (Nov 2014)
- Guidance for independent schools, academies and free schools (Nov 2013)

### Documents about the government's strategies to prevent terrorism and radicalisation

Prevent strategy:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

Channel guidance: https://www.gov.uk/government/publications/channel-guidance (Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.)

### Further support

- Earlier this year the Department for Education set up a telephone helpline (020 7340 7264) and an email address (counter.extremism@education.gsi.gov.uk) to enable people to raise concerns directly with the department.
- If you have a concern about a child in respect of extremism and the support options are not available locally, talk to your LSCB police representative or PREVENT coordinator who will be able to discuss support options.
- If you have a digital safety concern then please contact **The UK Safer Internet Centre's** Professionals Online Safety Helpline on 0844 381 4772 or helpline@saferinternet.org.uk

### Reporting online content

- Report terrorism related content to the police's Counter Terrorism Internet Referral Unit at www.gov.uk/report-terrorism.
- You can also refer content of concern directly to social media platforms - find out how http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/safety-features

### Training

For more information about the Home Office's radicalisation awareness training product Workshop to Raise Awareness of Prevent (WRAP) email WRAP@homeoffice.x.gsi.gov.uk

### Reporting to the police

**999** or your **local police**

Call the **Anti-Terrorist Hotline** on 0800 789 321 if you suspect someone is involved in terrorism in any way

Contact **CEOP** is you have any concerns regarding grooming http://ceop.police.uk/

Contact **True Vision** If someone is being targeted on the grounds of their religion, race, sexual orientation, transgender identity or disability http://www.report-it.org.uk/home

If you have any questions about the Trust Me resource then please feel free to contact Childnet by email at: **education@childnet.com**

**If you wish to give any feedback on the resource then please take a few moments to complete the online feedback form: www.surveymonkey.com/r/childnet-trustme**



By Childnet – CC – BY –NC – SA 4.0