At The National College, our WakeUpWednesday guides empower and equip parents, carers and educators with the confidence and practical skills to be able to have informed and age-appropriate conversations with children about online safety, mental health and wellbeing, and climate change. For further guides, hints and tips, please visit nationalcollege.com.

What Parents & Educators Need to Know about

DOXING

Doxing, or 'doxxing' (short for 'dropping documents'), is when someone's personal information is shared without their consent. This could include their phone number, home address, place of work or study, or sensitive information about their family, health, or other private matters. According to Ofcom, 5% of UK 13- to 17-year-olds say they've seen or experienced doxing online. It's often a malicious act and, depending on the circumstances, may be a crime.

WHAT ARE THE RISKS?

REPEAT OR MULTIPLE ATTACKS

Doxing is rarely a one-off incident. Information may be shared across multiple sites or groups, meaning an instance of doxing can escalate quickly. Some victims experience targeted, coordinated campaigns instigated by several people at once, which can feel overwhelming. Even when the information is successfully removed from online platforms, it may reappear on different accounts or sites, making it difficult to escape repeated harassment.

CAMPAIGNS OF CONTROL

Doxing, or the threat of it, can be used to manipulate and control victims. It's a known tactic used by cybercriminals to exploit young people online and can also be used to punish or control victims of domestic abuse. Blackmail, threats, harassment, stalking, and coercive control can constitute criminal offences, so incidents may need to be reported to the police.

MENTAL HEALTH IMPACTS

Doxing is linked to mental health risks, including stress, depression, and anxiety. Having sensitive personal information exposed online can feel violating, leaving victims feeling powerless. Doxing can also be seen as an 'invitation' for others to harass or 'pile on' to a target, making them feel increasingly vulnerable. Victims may need support and safe spaces to discuss the impact of a doxing campaign on their wellbeing.

UNEQUAL IMPACTS

Doxing can disproportionately affect those who are already marginalised, including women and girls, racially minoritised groups, LGBTQ+ people, those with disabilities or health conditions, and people from lower socioeconomic backgrounds. While anyone can be a victim, research shows that women are more likely to experience image-based or sexualised harassment and online 'mobbing' alongside doxing. One study found that 10% of young women aged 16 to 24 reported being doxed.

OFFLINE RISKS

When doxing reveals someone's location or address, it can put them at risk of offline harm or harassment. Victims may face vandalism, unwanted contact from strangers, being recorded or followed, or receiving items they did not ask for. Others living with them, such as family members, may also be at risk. Limiting the personal information available online can help reduce exposure, while harassment can be reported to the police.

CRIMINAL CONSEQUENCES

There are risks for those who take part in doxing, too. Under UK law, teenagers have been prosecuted for targeting other young people online. 'Swatting', which involves making false emergency reports to trigger an armed police response, is also linked to doxing and can be a criminal offence. Hacking into others' online accounts is illegal, too. Young people need to understand what constitutes a crime online and where to seek advice.

Advice for Parents & Educators

KNOW THE LAW

Doxing sometimes overlaps with criminal offences, including hacking, harassment, stalking, threats, coercive control, exploitation, blackmail, and image-based abuse. Depending on the circumstances, some victims may also have grounds to bring legal action against the misuse of their private information. Make sure that young people understand the potential legal consequences, both as victims and perpetrators, and contact the police about any suspected criminal activity.

ACT SWIFTLY

If a child or young person has experienced doxing, take it seriously and act quickly. Keep a record of the posts and accounts involved, report the doxing content to the platform, and consider whether temporarily limiting account activity could help. Seek advice from online safety organisations such as Internet Matters or CEOP and report any criminal activity to the police. In educational settings, follow safeguarding procedures. Signpost young people to Childline or The Mix for confidential support.

EXPLORE PRIVACY SETTINGS

Talk through the various digital privacy and security settings available online with young people. Show them how to make their accounts private, limit who can see their posts or contact them, and manage any location sharing settings. Encourage them to review these settings regularly, particularly when joining new platforms, to help them stay in control of their personal information and reduce the risk of being doxed.

TALK INFORMATION SECURITY

Doxing becomes easier when a person's information security is weaker. Ask young people what might be unsafe or compromise their privacy when posting content publicly online. Parents and educators should likewise be cautious about what they share and should try to model good cybersecurity habits, such as updating their passwords and using two-factor authentication.

Meet Our Expert



Dr. Holly Powell-Jones is the founder of Online Media Law UK and a leading UK expert in media law, online safety and young people. Her PhD investigates youth understandings of criminal and legal risks in a digital context. She works in schools to provide award-winning education on the criminal, legal, and ethical considerations of rapidly advancing technologies.

See full reference list on our website

#WakeUpWednesday®

The National College®

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 18.11.2026