Oxford International Study Centre
individually designed study programmes in the heart of Oxford

E-Safety and Social Media Policy

Introduction

This policy is designed in recognition of the fact that the digital environment has changed hugely over the last ten, or even five, years. Whereas previously the message regarding safety online was an overly-cautious, unfamiliar attitude of ‘just don’t use technology’, the changing nature of online resources and growing reliance on these resources for teaching and learning dictates that a different attitude be taken. This policy recognises that digital technologies have become integral to the lives of children and young people, both within schools and outside school, that these technologies are powerful tools, which open up new opportunities for everyone, and that these technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. It recognises that young people **will** be using the internet, and aims to ensure that all students, and staff, should have safe access to the internet, as well as to offer guidance on how the internet can be used safely and securely to prevent young people endangering themselves.

OISC offers filtered access to the internet, both wirelessly and on school computers. Should staff become aware of any site that is accessible using OISC internet access, which they believe ought to be filtered, they should let senior management know of this immediately.

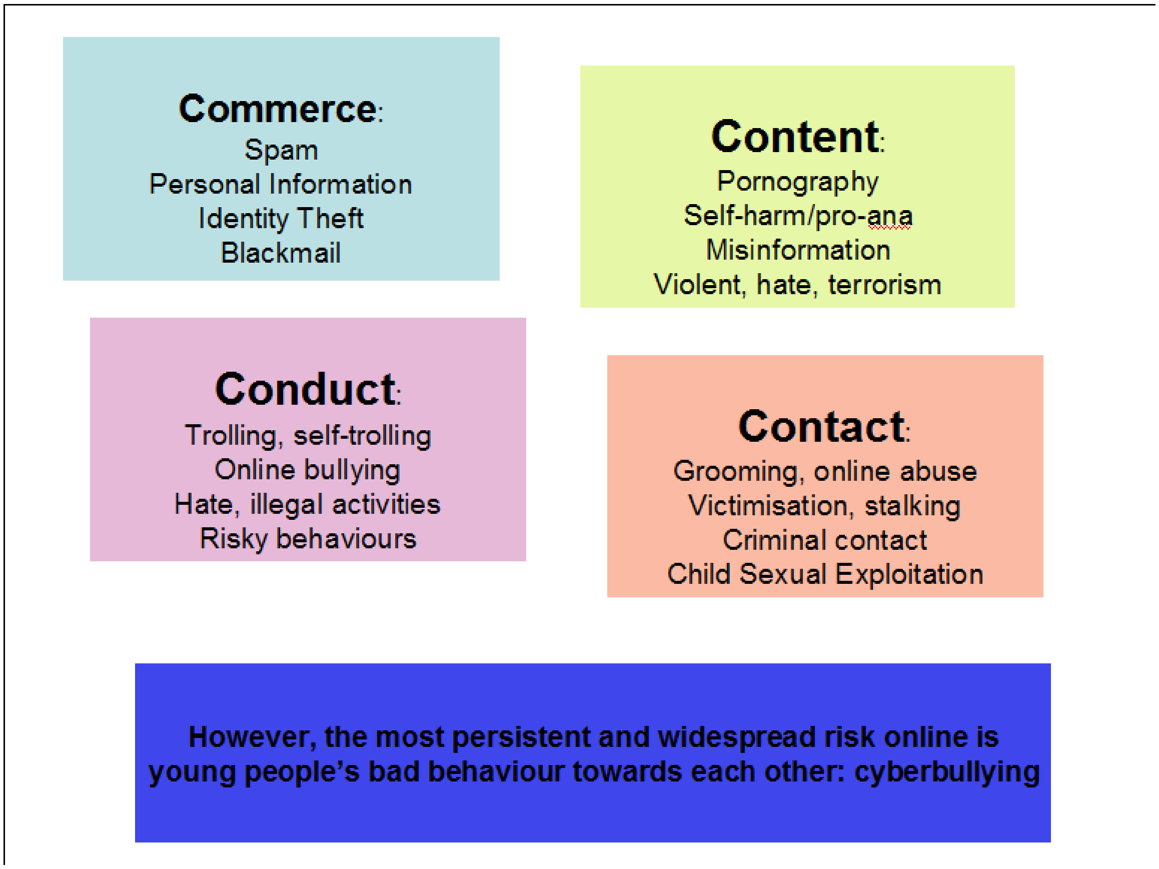
It is important to recognise that young people *are* online:

- 88% of households with children in the UK have internet access.
- This has decreased from 91% in 2013 – poorer households have been worst hit (74% now vs. 83% in 2013), while for richer households, internet access is near-universal (94% - 98%).
- 96% of young people aged 16-24 use a mobile phone or portable device of some kind to access the internet whilst on the move.

Young people are accessing content of many different types, both benign and potentially harmful:

- 3% of 5-7 year olds, 28% of 9-10 year olds, and 59% of 11-12 year olds have a social networking profile.
- 58% of 5-7 year olds, 68% of 8-11 year olds, and 59% of 12-15 year olds are playing computer or video games daily.

The majority of games, forums, social networking sites and other popular internet-based diversions are safe spaces which young people use to interact in a positive way. However, it is important to understand that all young people are at risk of abuse whilst using the internet. Internet abuse can, broadly speaking, be separated into four categories:



Commerce:
Spam
Personal Information
Identity Theft
Blackmail

Content:
Pornography
Self-harm/pro-ana
Misinformation
Violent, hate, terrorism

Conduct:
Trolling, self-trolling
Online bullying
Hate, illegal activities
Risky behaviours

Contact:
Grooming, online abuse
Victimisation, stalking
Criminal contact
Child Sexual Exploitation

However, the most persistent and widespread risk online is young people's bad behaviour towards each other: cyberbullying

Staff should be vigilant towards any behaviour, attitude or personal indicators that students might be subject to, or particularly at risk of, any of the above categories of online abuse. In particular, staff should be aware that the following groups of young people are particularly vulnerable to online abuse:

- Young people with a heavy investment in their online life, or a lot of online assets
- Young people already engaging in commercial or grey legal activity online
- Young people with LDD
- Young people who are LGBTQIA+
- Young people who are overtly sexually curious at an early age
- Young people with conduct issues or at risk of offending
- Young people who have overly controlling, or overly lax parental boundaries

Originally issued: April 2015
This version: September 2020
Last Reviewed: October 2021

Just as with safeguarding monitoring of all types, staff should be particularly vigilant in try to spot young people who seem to have established a ‘new norm’ when it comes to use of the internet.

In line with the college’s obligation to protect its students, and staff, in their safe use of the internet, staff agree to the following:

- I understand that OISC may monitor my use of the systems, devices and digital communications.
- I will be aware of “stranger danger”, when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me, or might make students, feel uncomfortable when I see it on-line. This can be done using the Click CEOP tool, the Internet Watch Foundation (IWF)

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

I will act as I expect others to act toward me:

- I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I □ecognize that OISC has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the college*:*

I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

Originally issued: April 2015
This version: September 2020
Last Reviewed: October 2021

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened. I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, even when I am not on college premises, where they involve my membership of the college community (examples would be cyber-bullying, use of images or personal information, or inappropriate relationships on social media).

•I understand that if I fail to comply with this policy, I will be subject to disciplinary action. This may be loss of access to the college network / internet, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Sexting

OISC recognises that the sending of inappropriate text messages and images (or ‘sexting’) is a significant cause for concern in the digital age, and can be extremely damaging to young people. When handling incidents involving sexting, senior management and the DSL will refer to the UK Council for Child Internet Safety (UKCCIS) document ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ for guidance. Where an incident of this nature is brought to the attention of the DSL, the Sexting Risk Assessment Tool, produced by CEOP and held on file, will be used to assess the risks involved, and to identify the appropriate course of action.

Online Teaching and Learning

Given the recent and significant increase in online teaching, due to ongoing impacts of Covid-19, it is important that tutors and students recognise their responsibilities in ensuring that online teaching and learning are undertaken effectively, and responsibly.

Tutors and Parents/Agents are therefore advised to consult the *Online Teaching Policy*, and students should refer to the *Guide to Online Learning* for advice and guidance.

Social Media and Professional Boundaries

For the purposes of this policy, and of all policies, the definition of a college student is a current or past student, irrespective of age. 'Past' is understood as covering a period of the student's leaving date, plus six months.

This social media policy is designed not to indicate suspicion of staff, but as part of the college's wider responsibility to safeguard both staff and students.

However much long-term students might come to be respected and admired, they are not friends. If we come to think of a student as a friend, a line has already been crossed. Staff should be quite clear on this and should act accordingly on social media just as they would in real life.

The Department for Education offers the following three key rules for social media use by staff:

- Keep personal information private
- Consider the long-term implications of content posted online
- Do not post inappropriate, offensive, or illegal content to your own or other online spaces

Furthermore, all members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006, and other legislation. They must also operate in line with the college's Equal Opportunities and Safeguarding & Child Protection Policies.

Staff are encouraged to act according to the following general guidelines in their social media use:

- Staff will not invite, accept, or engage in communications with parents or students from the college community on any personal social media profiles.
- Any communication received from students on personal social media sites should be reported to the Designated Senior Person (Ben Llewelyn), regardless of content.
- If any member of staff is aware of any inappropriate communications involving any child in social media, these must be reported immediately.
- Members of staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.

Originally issued: April 2015
This version: September 2020
Last Reviewed: October 2021

- Staff should not post on any social media with specific reference to individuals, or individual events occurring at OISC.

Useful E-Safety Resources

Click CEOP / CEOP Command - https://ceop.police.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

NSPCC: Online Safety –
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

CEOP Think U Know - https://www.thinkuknow.co.uk/

Government 'This is Abuse' Discussion Guide (archived 2016) -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/506536/Discussion_Guide_-_This_is_Abuse_update_July15_v2_Final.pdf

Oxfordshire Resources

- Anti-Bullying Web Pages including resources for cyberbullying and e-safety http://schools.oxfordshire.gov.uk/cms/content/anti-bullying follow link to internetsafety and cyberbullying
- Oxfordshire E-safety and Cyberbullying toolkit - updated January 2015 (pdf format, 314Kb)Oxfordshire information and guidance to support you to address e-safety and cyberbullying with young people. Provides links to local and national resources.
- Oxfordshire Duty Team http://www.oxfordshire.gov.uk/cms/content/report-child-abuse
- Plus general advice and information www.oxfordshire.gov.uk/cms/public-site/keeping-children-safe
- Oxfordshire Safeguarding Children Board - www.oscb.org.uk

National Resources

- **Childnet International** http://www.childnet.com/resources
- **Stop it now** (child sexual abuse prevention campaign, for all adults) www.stopitnow.org.uk and Parents Protect www.parentsprotect.co.uk
- **E-Safety self review tools provided by South West Grid for Learning** www.360safe.org.uk schools/ www.onlinecompass.org.uk youth settings
- http://accidentaloutlaw.knowthenet.org.uk/ Excellent quiz on internet + law
- **Internet Watch Foundation (IWF)** www.iwf.org.uk was set up by the UK internet industry to provide the UK internet 'Hotline' for the public to report potentially illegal online content.
- **CBBC Stay Safe** www.bbc.co.uk/cbbc/topics/stay-safe

Originally issued: April 2015
This version: September 2020
Last Reviewed: October 2021

- **Sexting** and support around self-generated images. Sexting in Schools: advice and support around self-generated images. What to do and how to handle it. and **for younger children:** NSPCC Share Aware campaign www.nspcc.org.uk/ShareAware including advice about how to keep safe online
- **ASK.FM** http://www.saferinternet.org.uk/ufiles/ASK.FM-fact-sheet.pdf
- **Web Cam fact sheet** http://www.thinkuknow.co.uk/Documents/Webcam%20fact%20sheet%202.pdf
- **Stonewall Guide** www.stonewall.org.uk/safeonline online risks to LGBT young people and how to support them to keep safe for professionals and parents/carers
- **O2 and NSPCC Parent/Carer Helpline** 0808 800 5002 http://www.o2.co.uk/help/nspcc

Report it:

- **Thames Valley Police** – for suspected criminal activity http://www.thamesvalley.police.uk/reptcr/reptcr-repform.htm
- **Oxfordshire County Council website** – for child safeguarding concern http://www.oxfordshire.gov.uk/cms/public-site/child-social-care
- **CEOP** – report a child in danger of abuse. Children can self-report. http://www.ceop.police.uk/safety-centre/
- **Internet Watch Foundation** – report child sexual abuse content http://www.iwf.org.uk/

Professionals Online Safety Helpline – 0844 3814772 helpline@saferinternet.org.uk

On-line Risky Behaviours Workshop – film list

http://www.channel4.com/programmes/goks-teens-the-naked-truth/articles/games-and-stuff Link to a number of cyberbullying clips – the site also has general resources on bullying and body image

Consequences about a young man becoming an online abuser. Focus on reporting. http://www.thinkuknow.co.uk/11_16/everything-else/films

First2amillion interactive film series about an internet bet that spirals out of control, focus on choice, character testimonies http://www.thinkuknow.co.uk/first2amillion/

Exposed – a video about the dangers of sexting. Focus on resilience. https://www.thinkuknow.co.uk/teachers/exposed/

Exploited – looks at risks of teenage behaviour, focus on disorganised/abusive relationships https://www.thinkuknow.co.uk/Teachers/Exploited/

Day Dreaming – Cyberbullying film clip for primary schools with resources and teachers notes *www.yhgfl.net › eSafeguarding › eSafety › Cyberbullying*

Digital Dirt – engaging short film about bad behaviour online affecting your job-seeking prospects http://youtu.be/JJfw3xt4emY

Caught in the Web – Newsround– 15 min video about grooming with a comforting narration and no distressing content http://www.bbc.co.uk/newsround/13908828

Online Bullying cyberbullying section from Newsround "Caught in the Web", short and impactful
http://www.youtube.com/watch?v=0XgLqTfM-1I

The Anti-Social Network http://www.eastlandsprimaryschool.co.uk/e-safety/the-anti-social-network film made by Year 5 at Eastlands Primary School about cyberbullying and E-safety.
School website has good links for parents and children.

Stop it now – 60s brief video (no distressing content) raising awareness of child sexual abuse from Stop it now! http://www.stopitnow.org.uk/60_secon_video.htm

Parents protect! – 30 minute educational video for parents and carers, mythbusting and thorough, includes testimonies http://www.parentsprotect.co.uk/video.htm