

# Online Safety Policy

Roselyn House School

2026 – 2027



|                     |                 |                         |
|---------------------|-----------------|-------------------------|
| <b>Approved by:</b> | Jack Birkenhead | <b>Date:</b> 17/07/2026 |
|---------------------|-----------------|-------------------------|

|                          |           |
|--------------------------|-----------|
| <b>Last reviewed on:</b> | July 2026 |
|--------------------------|-----------|

|                            |           |
|----------------------------|-----------|
| <b>Next review due by:</b> | July 2027 |
|----------------------------|-----------|

## 1. Introduction

Online learning is now an established part of the Roselyn House School curriculum and may also be used to support students who are absent due to illness but well enough to continue learning. This Policy has been revised to follow DfE Keeping Children Safe in Education (KCSiE) 2026 and guidance from the Children's Safeguarding Assurance Partnership (CSAP), previously Lancashire's Safeguarding Children's Board. It should be read in conjunction with Roselyn House School's Safeguarding Policy, Remote Learning Policy, Cyber Security Standards audit, Security Policy, Emergency Planning and Procedures Policy, Behaviour Policy and Mobile Phone Policy.

Roselyn House School adjusted the way learning could take place in the event of a student having to be absent due to illness but is well enough to continue education. This is to ensure every student has the opportunity to continue with education during this time. Remote learning will be used as a tool to educate the students consistently during any sporadic school closures or if an individual is unable to attend school. Remote learning should be followed in accordance with the Online Safety Policy.

Online Safety may be described as Roselyn House School ability to:

- Protect and educate pupils and staff in their use of technology.
- Have the appropriate mechanisms to intervene and support any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material, for example; pornography, fake news, racist or radical and extremist views.
- Contact: being subjected to harmful online interaction with other users for example commercial advertising as well as adults posing as children or young adults; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

The '3C's Risk Matrix' was originally identified through the LSE 'EU Kids Online' project and is a useful means of categorising risk areas according to type. In addition, a fourth risk areas sometimes used to include 'Commercial' – referring to risks around financial or data related issues (e.g. harvesting of personal information for financial purposes). It is important to recognise that these risk areas are not mutually exclusive (e.g. extremist content can also apply to 'conduct' as well as 'content.'

The range of online issues is broad and complex and forever changing, The Little Big Book of Online Safety terms is a useful resource to explain some common terms.

<https://www.safeguardingpartnership.org.uk/online/resources/>

Online Safety is primarily a Safeguarding issue and therefore the responsibility for Online Safety falls within the remit of the Designated Safeguarding Lead. Remote Learning Policy and Safety has been specifically designated within the school.

Addressing effective Online Safety requires a collaborative, whole school approach. Therefore, staff with appropriate skills, interest and expertise should be encouraged to support the DSL's, for example when developing curriculum approaches or making technical decisions.

Where an online safety incident raises safeguarding concerns, including concerns about exploitation, coercion, harmful online contact, repeated incidents or a student's welfare, this will be reported and recorded in accordance with the school's Safeguarding and Child Protection Policy and Keeping Children Safe in Education (KCSiE) 2026. Where appropriate, a CPOMS record will be completed and reviewed by the Designated Safeguarding Lead.

## **2. Why is Internet use important?**

- The purpose of Internet use in Roselyn House School is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance our management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff, students and parents/ carers.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is available to support communication internally and externally.
- The Internet is an essential element in 21st century life for education, business and social interaction. Roselyn House School has a duty to provide students with quality Internet access as part of their learning experience.
- Provides the opportunity of remote learning for students unable to attend Roselyn House School's premises. (See Remote Learning Policy)

## **3. How does the Internet benefit education?**

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries.
- Inclusion in government initiatives such as the DfE ICT in Schools and the Virtual Teacher Centre (VTC) <http://vtc.ngfl.gov.uk>, Oak Learning Academy and many other online resources which have recently been developed to enhance or take the place of classroom learning.
- Educational and cultural exchanges between students worldwide- Roselyn House School is linked with Hope Flowers, Bethlehem.
- Cultural, vocational, social and leisure use in libraries, clubs and at home.

- Access to experts in many fields for students and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the LEAs and DFE.
- Mentoring of students and provide peer support for them and teachers
- Ensuring ongoing education for those students who are unable to attend school.

#### **4. How can Internet use enhance learning?**

- Roselyn House School's internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Can be used where appropriate to deliver online lessons.

Effective Online Safety education should be embedded across the curriculum, including PSHE. It is important for Teachers to identify and reference ways that online aspects of Safeguarding can be reinforced in their respective lesson planning and delivery. For example, when different subjects utilise technology as Teaching and Learning tools.

Roselyn House School Online Safety Curriculum should be flexible, relevant, engage student's interests, be appropriate to their own needs and abilities and encourage students to develop resilience to online risks. Staff should be mindful that Online Safety resources can become dated very quickly and keep as up to date as possible.

Given the school's specialist SEMH context, staff should be alert to online risk-taking behaviours, impulsive online activity, online coercion, county lines recruitment, online gambling, harmful online communities, self-harm content, suicide forums, eating disorder material, harmful online challenges and online peer pressure. Concerns should be treated as safeguarding concerns and recorded in line with school procedures.

Delivery of the Online Safety Curriculum could include student council and elements of peer education.

## **5. How will students learn to evaluate Internet content?**

- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-ordinator and/or the Head Teacher or Deputy Head Teacher (s).
- Roselyn House School will ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Online Safety should also be taught discreetly and provides the opportunity to encompass specific aspects the school may encounter or address concerns students may have raised. Developing Digital Literacy remains a key aspect in supporting Children and Young People and building their resilience to online issues, both in recognising risks and developing their own online behaviour.

Young people with special educational needs and disabilities can be particularly vulnerable to the risks posed by online interaction. Discussion around our students is paramount to determine who may be at higher risk and a whole school approach and training for staff is vital in supporting our students' safety.

Staff are trained in Safeguarding on induction and then annually. There is also specific training for Online Safety and Cyber Crime.

Staff training will include annual online safety updates, KCSiE updates, cyber security awareness, phishing awareness, filtering and monitoring awareness, social media safety and awareness of emerging technologies including artificial intelligence. The Designated Safeguarding Lead will undertake additional training relating to online safety risks, online exploitation, cybercrime, harmful online content and emerging technologies.

[https://blackburn.melearning.university/course\\_centre/course\\_details/53](https://blackburn.melearning.university/course_centre/course_details/53)

[cyber security training for school staff](#)

(NCSC Training)

Staff also receive regular CSAP 7-minute briefings throughout the year.

Social Media can be particularly challenging for our students and helping them to navigate more safely should be a key aspect of the Online Curriculum. See also Social Media Policy.

The responsibility of the proprietors of KS Education Limited is to ensure that Online Safety is part of school safeguarding responsibilities and that the increasing role of the online environment within safeguarding provision is evident in school policy. Supporting tools such as internet content filters and monitoring systems are in place. It is essential to recognise that whilst these are important supporting tools, they are

not a solution and should be implemented to support and complement effective classroom practice and appropriate student behaviour as part of a wider holistic approach to managing online access. In KCSiE 2026, this includes keeping children safe online when at home.

Safeguarding considerations need to be met when students are without the physical structure of attending school and parents/ carers should be informed of how to help keep their children safe. There is DfE Guidance published which is sent to Parents. Please see Remote Learning Policy.

## **6. How will e-mail be managed?**

- If they have a Roselyn House School email, students may only use approved e-mail accounts on the school system after permission has been sought.
- Students must immediately tell a staff member if they receive offensive e-mail.
- Students must not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on Roselyn House School headed paper.
- The forwarding of chain letters is not permitted.

## **7. How should Web site content be managed?**

- The point of contact on the Web site should be the Roselyn House School address, e-mail and telephone number. Staff or students' home information will not be published.
- Web site photographs that include students will be selected carefully and written permission from parents or carers will be obtained before photographs of students are published on Roselyn House School websites.
- Students' full names will not be used anywhere on the websites, particularly in association with photographs.
- The Head Teacher, and/ or the Deputy Head Teacher(s) will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with Roselyn House School's guidelines for publications.
- The copyright of all material must be held by Roselyn House School or be attributed to the owner where permission to reproduce has been obtained.

## **8. Chat Rooms and Social Media**

- Students nor staff will not be allowed access to any kind of chat rooms.
- No students or staff will be permitted to use social media unless permission has been granted by parents/ carers (students) and by the Headteacher or Deputy Headteacher (s).

- (See Social Media Policy)

## **9. New Technologies**

- Emerging technologies will be examined for educational benefit before use at Roselyn House School is allowed.
- Students may bring mobile phones to school, as we understand that these are a source of attachment to family members but they will not be used during lessons or formal school time unless authorised or for educational purposes (For example TEAMS chats).
- The sending of abusive or inappropriate text messages/ private messaging is forbidden. The school will follow procedures outlined in the Behaviour Policy and Anti-Bullying Policy.
- A risk assessment will be carried out before students are allowed to use a new technology in school.
- Generative artificial intelligence tools, including systems such as ChatGPT, Microsoft Copilot and similar platforms, will only be used where this has been risk assessed and authorised by senior leaders. Staff and students must not enter personal, confidential or safeguarding information into AI tools. Students will be supported to understand the risks of misinformation, bias, plagiarism, inappropriate content and AI-generated images or text.

## **10. Online tutoring**

In light of students having to switch to remote learning; online video tutoring may be used to replace in class learning or enhance the education of students.

- Written consent must be received before lesson can take place.
- Only SLT approved systems will be used.
- Only Roselyn House School registered staff accounts will be used.
- A member of SLT must be made aware of a lesson taking place before commencing.
- One-to-ones will be avoided unless pre-approved by SLT.
- Where possible another member of staff will be present on the call.
- If no staff available a digital audio recording of the lesson will be made and securely, remotely stored in line with GDPR.
- Throughout the duration of a virtual session, a responsible adult must be present with the student.
- Video calls can only take place in appropriate places with consideration of the background image, no inappropriate objects/information visible.
- Staff and children must wear suitable clothing.
- A record will be maintained of attendees for each lesson.
- The Remote Learning Policy must be followed.

## **11. Roselyn House School Official Social Media Accounts and Digital Communication Platforms**

Roselyn House School official social media accounts and future digital communication platforms are for appropriate communication with students past and present, parents/carers and the wider school community. Private messaging will be monitored by authorised senior staff and the IT Manager only. Inappropriate messages or comments will be reported, removed where necessary and recorded in line with safeguarding procedures. No staff personal accounts will be added or used for school communication.

Content posted to official school channels will be approved by the Proprietors, Headteacher or delegated senior leader and reviewed regularly to ensure it remains accurate, appropriate and safe.

## **12. You Tube**

Any videos produced by staff will be posted to Roselyn House School's You Tube account and are for the use of learning and wellbeing. The comment section will be disabled and the views monitored and reported if not appropriate. All content will be approved by the Headteacher before being posted.

## **13. How will Internet access be authorised?**

- Roselyn House School will keep a record of all staff and students who are granted Internet access. The record will be kept up to date, for instance a member of staff may leave or a student's access be withdrawn.
- Our students must apply for Internet access individually by agreeing to abide by the Responsible Internet Use statement.
- All students and staff who attend Roselyn House School must abide by the Responsible Internet Use statement.
- Parents/Carers will be asked to sign and return a consent form.

## **14. How will the risks be assessed?**

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. Roselyn House School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Roselyn House School cannot accept liability for the material accessed, or any consequences of Internet access that is beyond the school's current filtering system.

Other common risks include:

## **15. Content**

- Exposure to inappropriate content, including online pornography; ignoring age ratings in games (exposure to violence, often associated with racist language); and substance abuse.
- Lifestyle websites, for example pro-anorexia, self-harm or suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

## **16. Contact**

- Grooming.
- Child Sexual Exploitation and Child Criminal Exploitation. CSE in particular may involve using the Internet and social media to identify potential victims or as a tool to coerce or blackmail children into performing sexual acts both online and offline. Means of using the Internet may also be provided in the form of a gift by perpetrators in the form of phones and devices. Some CSE can take place entirely online and may not always been a physical meeting between victim and offender. DSL's should be aware of local guidance for CSE and include in Safeguarding that it can happen online also. CEOP has some useful resources.
- Cyber-bullying in all forms.
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.
- Radicalisation- there is an increasing role through the Internet and social Media as tools in the radicalisation of young people. Online grooming and radicalisation can be conducted in very similar ways. All Schools have The Prevent Duty under section 26 of the Counterterrorism and Security Act 2015.

## **17. Conduct**

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online (internet or gaming)).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)- (any disclosure should follow Roselyn House School's normal safeguarding practices and protocols. ("Sexting" in schools - advice and support around self generated images- see [parentsprotect.co.uk](http://parentsprotect.co.uk) and UKCIS Sexting Advice).
- Child on child abuse, sexual violence and sexual harassment between young people can include a significant number of online elements. These can take place between children of any age, sex and gender and may include groups of

children harassing a single child or group. Additionally, it includes reference to particular groups being potentially more at risk such as girls, children with SEND and LGBT+ children. Within the definitions of sexual harassment there is specific reference to online sexual harassment including non-consensual sharing of images/ videos, sexualised online bullying, sexualised comments on social media and sexual exploitation through coercion and threats.

- Upskirting is an illegal act which involves the use of a device to take a photograph or video under a subject's clothing without their knowledge for the use of sexual gratification or to cause harm. This then can be posted online.
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- KCSiE 2025 highlights the need for protection in relation to publicity for the alleged perpetrator and victim. This is particularly relevant where students may circulate information via social media. It is worth noting the Internet Watch Foundation who may be able to support removing illegal images.
- Online sexual abuse may also include deepfake imagery, AI-generated sexual images, image-based abuse, online coercion, blackmail and sextortion. Any concern of this nature must be managed as a safeguarding concern and referred to the Designated Safeguarding Lead.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher and Online Safety Team will ensure that the Online Safety policy is implemented and compliance with the policy monitored.

### **18. Why is this important?**

Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and students are using technology at an ever earlier age.

### **19. How will filtering be managed?**

- Blocking strategies prevent access to a list of unsuitable sites or newsgroups.
- Maintenance of the blocking list is a major task as new sites appear every day.
- A walled-garden or allow list provides access only to a list of approved sites. An allow list will inevitably restrict students' access to a narrow range of information.
- Dynamic filtering examines the content of Web pages or e-mail for unsuitable words. Filtering of outgoing information such as Web searches is also required.
- Rating systems give each Web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.

- Monitoring records Internet sites visited by individual user. Access to a site forbidden by the filtering policy will result in a report. It is also possible to remove access automatically after a set number of policy violations.
- Roselyn House School will work in partnership with parents/ carers, the LEA, DFE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-ordinator
- Senior staff and the ICT Co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that Roselyn House School believes is illegal must be referred to the Internet Watch Foundation (please see references given later).
- Filtering strategies will be selected by Roselyn House School, in discussion with the filtering provider. The filtering strategy will be selected to suit the age and curriculum requirements of the student.

## **20. Web Filtering**

Roselyn House School utilises an internet filtering facility provided by Rawstream Ltd. The web filtering service provides the ICT Manager with a web interface with which they can control and monitor internet usage in both school sites. The web interface is accessed at least once a week by the ICT Manager to ensure unsuitable URLs are not being accessed, that attempted access is reviewed, and that appropriate action is taken to prevent further breaches. Filtering and monitoring reports will be reviewed regularly by the Designated Safeguarding Lead, Headteacher and ICT Manager so that emerging safeguarding concerns are identified and acted on promptly. The software allows for blocking categories such as social media, adult content, Chat Rooms and Drug use, amongst many others. It also provides blocking for Virtual Private Networks (VPNs), search engine filtering and filtered YouTube access to support age-appropriate use. The web filter is active on both the Wired Local Area Network and over the WiFi access points.

## **21. How will the policy be introduced to students?**

- Rules for Internet access and Responsible Internet Use will be posted in all rooms where computers are used.
- Students will be informed during induction and reminded regularly that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Students will look at Online safety across the curriculum including PSHE.
- Roselyn House School will have open discussion with students about online safety so that students learn to set personal boundaries and feel more comfortable reporting incidents like bullying and harassment.

## **22. How will staff be consulted?**

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource at Roselyn House School.
- All staff including teachers, supply staff, learning support assistants and auxiliary staff, will be provided with the Online Safety Policy and sign to say they have read it.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible Internet use and on the school e-safety policy will be provided as required.
- Staff should read and adhere to the Electronic Information and Communications Systems, Remote Learning, E-Safety and Social Media Policies.

## **23. How will ICT system security be maintained?**

Local Area Network security issues include:

- The user must act reasonably. Loading non-approved software could cause major problems. Good password practice is required including logout after use.
- The workstation should be secure from casual mistakes by the user.
- Cabling should be secure and wireless LANs safe from interception.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured to a high level.
- Virus protection for the whole network must be installed and current.
- Multi-factor authentication, strong password management, phishing awareness, secure use of personal devices and prompt reporting of suspected data breaches will form part of the school's cyber security arrangements.

Wide Area Network (WAN) security issues include:

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into Roselyn House School without specific permission from the ICT Co-ordinator and Head Teacher or Deputy Head Teacher (s) and a virus check.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Files held on our network will be regularly checked.
- The ICT co-ordinator will ensure that the system has the capacity to take increased traffic caused by Internet use.
- All USB flash drives must be encrypted if they contain any confidential school content.

## **24. How will complaints regarding Internet use be handled?**

- Responsibility for handling incidents will be delegated to senior members of staff.
- Any complaint about staff misuse must be referred to the Headteacher or Deputy Headteacher (s)
- Students and parents/ carers will be informed of the complaint's procedure.
- Parents/ carers and students will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include interview/ counselling by the Headteacher or Deputy Headteacher (s) or other Senior staff informing parents/ carers, removal of Internet or computer access for a period, which could prevent access to files held on the system, including examination coursework.

## **25. How will parents'/ carers' support be enlisted?**

- Parents'/ Carers' attention will be drawn to the Online Safety Policy in letters/ newsletters, the prospectus and on the Roselyn House School Websites.
- Internet issues will be handled sensitively to inform parents/ carers without undue alarm.
- A partnership approach with parents/ carers will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Interested parents/ carers will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).
- The following link is on the Roselyn House School website and included in consent forms for all parents/ carers to register for e-safety support.

<https://www.e-safetysupport.com/trainingcourses/17/training>

## **26. Internet Across the Community**

- Adult users will need to agree by the acceptable use policy.
- Parents/carers of children under 16 years of age will be required to sign an acceptable use policy on behalf of the child.
- In libraries, children under 8 years of age must be accompanied by an adult when accessing the Internet.

## **27. Monitoring Arrangements**

This document will be reviewed every year, but may be reviewed and updated more frequently if necessary. It will be reviewed by **Mr Jack Birkenhead** (*Headteacher*) in consultation with the wider school community.

## **28. Linked Policies**

This Policy is linked to the following policies and documents:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Restrictive Physical Intervention Policy
- Staff Code of Conduct
- Acceptable Use Agreements
- Data Protection Policy
- Remote Learning Policy

**References**  
**Particularly for Parents/ Carers and Children.**

**Keeping Children Safe in Education 2026**

For Schools and Colleges

[www.gov.uk/government/publications/keeping-children-safe-in-education--2](http://www.gov.uk/government/publications/keeping-children-safe-in-education--2)

**Teaching Online Safety in Schools January 2023**

[www.gov.uk/government/publications/teaching-online-safety-in-schools](http://www.gov.uk/government/publications/teaching-online-safety-in-schools)

**Bullying Online** [www.familylives.org.uk](http://www.familylives.org.uk)

Advice for children, parents and schools

**NSPCC**

[www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying/](http://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/bullying-and-cyberbullying/)

**UK Safer Internet Centre** [www.saferinternetday.org](http://www.saferinternetday.org)

**Parentsprotect** [parentsprotect.co.uk](http://parentsprotect.co.uk)

A guide for parents/ carers about potential dangers their children can face when using the internet.

**Childnet** [www.childnet.com](http://www.childnet.com)

An internet safety site from Childnet, with low-cost leaflets for parents.

**Connect Safely** [ConnectSafely.org](http://ConnectSafely.org)

Family guide to making Internet safe, fun and productive.

**Internet Watch Foundation** [www.iwf.org.uk](http://www.iwf.org.uk)

Reporting criminal online content

The following link provides access to a wide-ranging glossary of technological terms in current use: [www.childnet.com](http://www.childnet.com)

### Notes on the legal framework

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

#### Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

#### Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

#### Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent there is no need to prove any intent or purpose. GDPR/Data Protection Act 2018.

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers and must comply with

important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 — 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files).
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include Racist, Xenophobic and Homophobic comments, messages etc.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually, a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 — 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

This also includes incidents of Racism, Xenophobia and Homophobia.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess “extreme pornographic image”

63 (6) must be “grossly offensive, disgusting or otherwise obscene”

63 (7) this includes images of “threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead” must also be “explicit and realistic”

Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

- Headteachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.