Bradfield Online Safety Policy

Policy development:

This policy has been developed by building on our own best practice and that of other educational networks. It has been developed in consultation with Tapton Trust and is accessible through the Bradfield School website.

Governor Committee: Full Governing Body
Last ratified by Governors: January 2021
Due for review: January 2022
Senior leader responsible: Headteacher, Designated Safeguarding Lead, Designated Safeguarding Deputies, Head of ICT, Network Manager Ratified by Chair of Governors:

Online Safety Committee

- Head teacher
- Designated Safeguarding Lead
- Network Manager
- Head of Computer Science
- Safeguarding Governor
- Designated Safeguarding Deputies
- PSHE Co-ordinator

Contents

Background

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school Online Safety policy should help to ensure safe and appropriate use.

The use of digital technologies can put young people at risk within and outside the school, these risks include: access to harmful or inappropriate content, data breach, grooming, cyberbullying, copyright infringement and the potential for excessive use which may impact on the social and emotional development and learning of the young person.

The Online Safety policy that follows explains how we intend to manage and reduce these risks for all users.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems. This involves the use of the school system both within the school building and remotely.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying or other Online Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety.

Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school

Governors: Governors are responsible for the approval of the Online Safety Policy and for reviewing the policy. The role of the Online Safety Governor may include: • meetings with the Online Safety Co-ordinator • monitoring of Online Safety incident logs • monitoring of filtering / change control logs with the Network Manager • to report back to Governors	Headteacher and Senior Leaders: • are jointly responsible for ensuring online safety of members of the school community • are responsible for ensuring that staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant. • will monitor online activity via Smoothwall daily reports and will delegate this to the DSL in their absence. • are aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff
Online Safety Coordinator & Designated Safeguarding Lead: • leads the Online Safety committee • reviews the school Online Safety policies • provides annual training and advice for staff as needed • the DSL liaises with the Local Authority if needed and with school ICT technical staff • receives reports of Online Safety incidents and uses them to inform future developments • meets with Governor(s) to discuss current issues	Community Users: Community Users, such as Arches and the Sheffield Music Hub, who access school ICT systems as part of the Extended School provision will be expected to sign an AUP before being provided with access to school systems.
Parents / Carers • Parents and carers will be responsible for: • endorsing (by signature) the Pupil / Pupil Acceptable Use Policy • accessing the school website, on-line pupil records in accordance with the relevant school Acceptable Use Policy • the school will inform and update parents/carers about national / local Online Safety campaigns / literature.	Pupils: • are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems • are expected to behave sensibly should they come into contact with inappropriate material via the internet (should the filtering system fail) and report this to their teacher • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • will be expected to know school policies on the use of hand held devices including taking / use of images and on cyber-bullying

Online Safety Committee : Members of the Online Safety committee will assist in the area of Online Safety with: reviewing the school Online Safety policy and other related areas e.g. filtering	

Teaching and Support Staff :	Network Manager / Technical staff :
• have an up to date awareness of Online Safety including policy and practices, through annual CPD / new staff induction / briefing updates as necessary • report any suspected misuse or problem for investigation • digital communications with pupils e.g. email, should be professional and only carried out using official school systems • Online Safety issues are embedded in all aspects of the curriculum and other school activities. • A planned Online Safety programme will be provided as part of ICT/PSHE and other lessons • help pupils understand and follow the school Online Safety policy, through the role of form tutor, assemblies, pastoral activities etc • help pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations, helping them be critically aware of the accuracy of sources • monitor ICT activity in lessons, extra-curricular and extended school activities , including remote monitoring using AB Tutor. • are aware of Online Safety issues related to the use of hand held devices (phones, camera etc) and implement current school policies with regard to these devices • should act as good role models in their use of ICT, internet and mobile devices • know how to use the Behaviour Incident area of BromCom, with the option of Online ‘E’ safety being chosen for any incidents • in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use / where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit • it is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network can temporarily remove those sites from the filtered list for the period of study, or pre advise the Online Safety Coordinator checking the Smoothwall reports.	• ensure that the school’s ICT infrastructure is secure, with updated automated password protection • is informed of issues relating to the filtering applied by the Smoothwall • keeps up to date with Online Safety technical information and updates others as relevant • use of the internet, network and email is regularly monitored in order that any misuse or attempted misuse can be reported to relevant staff for investigation depending on the severity and background of the incident. • keep servers, wireless systems and cabling securely located and protected • provide users with clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed • an agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system. • ensure that the “administrator” passwords for the school ICT system must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe) • ensure that users will be made responsible for their password security and must immediately report any suspicion or evidence that there has been a breach • in the event of the Network Manager needing to switch off or alter the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader). • any filtering issues should be reported to the Network Manager and any requests to amend the system be considered by the Online Safety team • ensures that personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured • limit removable media to limit data breaches, memory USB sticks are not permitted, staff are given suitable cloud storage as • ensures that the Acceptable User Policy is updated and shared with all staff at relevant points

Library access - LRC

Pupils and staff may use the computers in the library on the 1st floor and breakout areas (eg outside Science) for internet access before, during and after school. These are supervised by staff when on duty. Pupils are expected to undertake educational work and games only and as such, follow the library working policy for PC use (as displayed in the library area).

Photos/Videos

Staff and pupils need to be aware that images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term, and staff/pupils need to know how to protect themselves from this:

- take care and know the risks when using digital images and publishing their own images on the internet e.g. on social networking sites
- staff are allowed to take digital video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- care should be taken when taking digital video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- pupils must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with guidance on the use of such images
- pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs unless prior consent has been granted by parent or carer
- written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- pupil's work can only be published with the permission of the pupil and parents or carers
- Staff must check BromCom photo permissions before posting / using images

Cloud Storage

Student/staffs will be given access to Office 365 and OneDrive (an online cloud storage resource), both in school and at home via an internet connection. Pupils/ staff must use it in a sensible manner or may have access restricted. Pupils/staff must be aware of and agree to the following:

- they will not type any form of libel, slander, profane or inappropriate, rude or suggestive language in any posts/newsfeed
- they will not upload any materials that could potentially harm the school network or that could be used for inappropriate use, remembering that the facility is provided for educational purposes only.
- they understand that their Office365 account and use of the system may be monitored at any time, and all usage is audited.

If any user violates any of these provisions, their access to the network will be terminated and all future access could possibly be denied and other appropriate actions may be taken.

Data Protection and Other Legislation

See separate Data Protection Policy and GDPR Policy for more information

There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Bring Your Own Device (BYOD)

It is not an expectation for staff/pupils to BYOD, but they can if they wish. However it is a privilege and not a right.

- where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- any device loss, theft, change of ownership of the device will be reported
- pupils wishing to BYOD – other devices, should do this in consultation with their HOY/parental discussion, SEND dept, ICT dept as required and acknowledge that the school is not liable for any damage / theft as users understand it is their choice to BYOD. Devices must be password protected.

Communications

For further advice on what is / is not allowed in terms of communication devices please refer to the table in Appendix 3

When using communication technologies:

- any digital communication between staff and pupils or parents / carers (email, chat, Office365 etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications

- whole class / group email addresses may be used. Pupils will be provided with individual school email addresses for educational use
- staff MUST NOT use their own phone for school business, but use the school systems or school provided mobile phones so that calls, messages etc are open and can be monitored to ensure the safety of all pupils and staff. In exceptional circumstances, staff can use their phone as long as their number is withheld to parents/carers.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyberbullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. For more information on these, please refer to the table in Appendix 4

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse: If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The DSL should be consulted, with a view to reporting the incident to the police and the preservation of evidence.

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Sexting

All incidents involving youth produced sexual imagery should be responded to in line with the school's safeguarding and child protection policy.

When an incident involving youth produced sexual imagery comes to a school or college's attention:

- The incident should be referred to the DSL as soon as possible
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately

Where one of the parties is over 18, this is no longer sexting but child sexual abuse.

Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

It is important that everyone understands that whilst sexting is illegal, pupils/pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

Cyberbullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying

See separate Bullying Policy for more information

Social Media - Protecting Professional Identity

School staff should ensure that:

- no reference should be made on personal social media accounts to pupils, parents / carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school or Multi Academy Trust.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

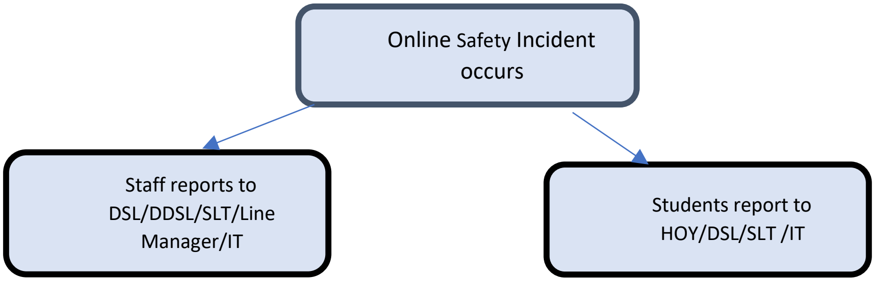
Illegal Incidents

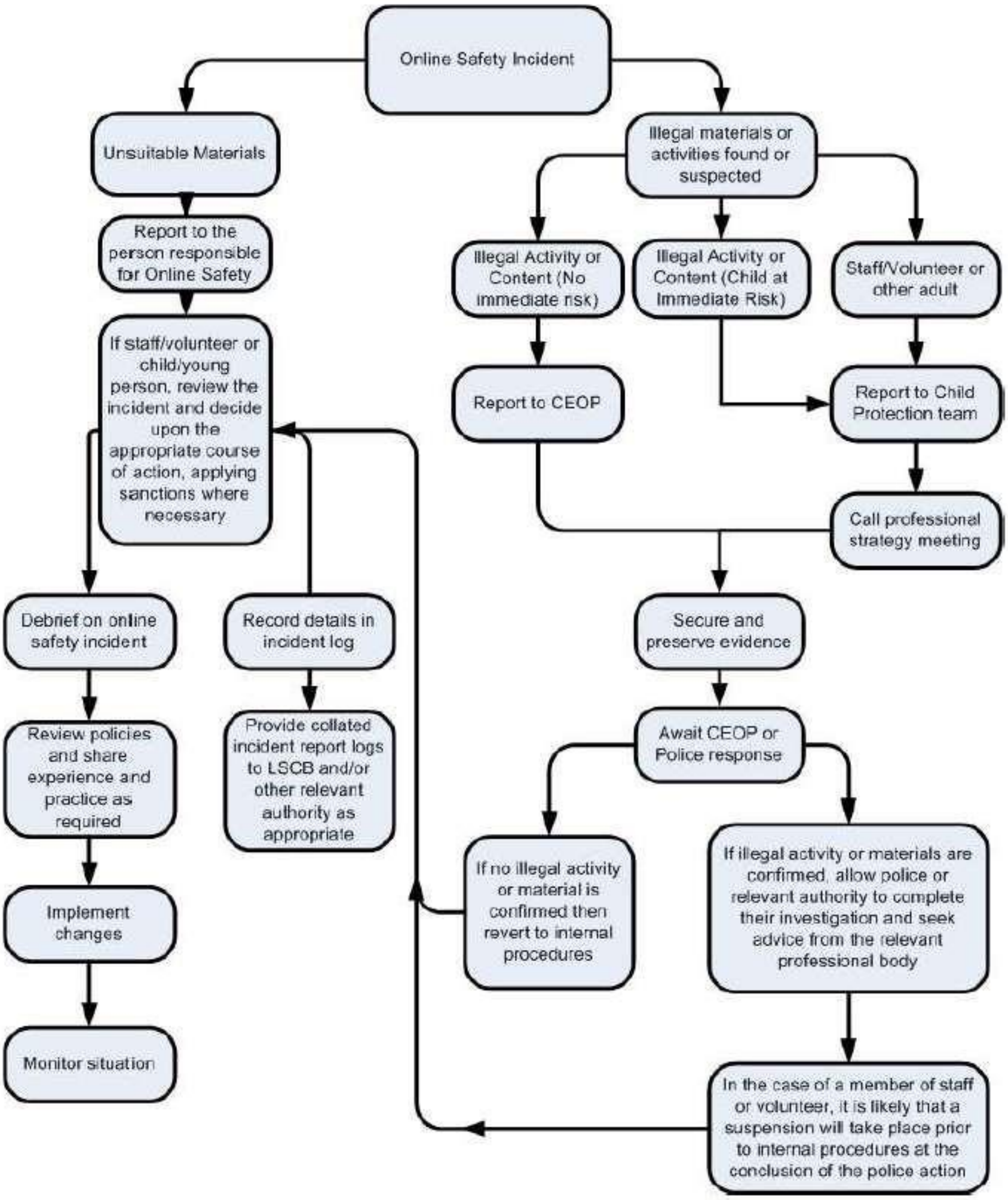
If there is any suspicion that a web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.

If in doubt, staff to speak to Helen Tyrrell, Lynn Wood or Tom Carrington (Safeguarding). Reports can be made internally via CPOMS

Follow the incident reporting flowchart on Page 11:

Incident Reporting Flowchart


Online Safety Incident occurs
Staff reports to DSL/DDSL/SLT/Line Manager/IT
Students report to HOY/DSL/SLT /IT


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

In the event of suspicion, all steps in this procedure should be followed:

- conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure. It is recommended that this is done via the IT Network Manager's office or SLT office.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the URL (website address) of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- if content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour or the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Actor criminally racist material
  - other criminal conduct, activity or materials
- isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendices

Appendix 1. Useful Links

The following sites as useful for providing further information:

NSPCC Netaware https://www.net-aware.org.uk/
Sheffield Safeguarding Children Board www.safeguardingsheffieldchildren.org.uk
Safer Internet Centre www.saferinternet.org.uk
UK Council for Child Internet Safety www.education.gov.uk/ukccis
CEOP think U Know www.thinkuknow.co.uk
Childnet www.childnet.com
Netsmartz www.netsmartz.org/index/aspx
Internet Watch Foundation – report criminal content www.iwf.org.uk
Guidance for safer working practices for adults that work with children and young people http://webarichive.nationalarchives.gov.uk/20100202100434/dcsf.gov.uk/everychildmatters/resourcesand-practice/ig00311/
Information Commissioners Office / education and ICO guidance on use of photos in schools www.ico.org.uk
Protecting your personal information online www.ico.org.uk
Getnetwise privacy guidance http://privacy.getnetwise.org/
External reporting sources: SWGfL BOOST includes an anonymous reporting app Whisper
http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper

For Parents / Children:

CEOP think U Know www.thinkuknow.co.uk
Safer Internet Centre www.saferinternet.org.uk
Vodafone Parents Guide http://parents.vodafone.com
NSPCC https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
Parent Zone www.parentinfo.org
Childnet http://www.childnet.com
Internet Matters www.internetmatters.org
CBBC Stay Safe www.bbc.co.uk/cbbc

Technology

CEOP report abuse button www.ceop.police.uk/Safer-By-Design/Report-abuse/
Internet Matters www.internetmatters.org
Get Safe Online www.getsafeonline.org
Microsoft Family Safety software http://windwos.microsoft.com/en-Us/windowsvista/Potectingyourkids-with-Family-Safety

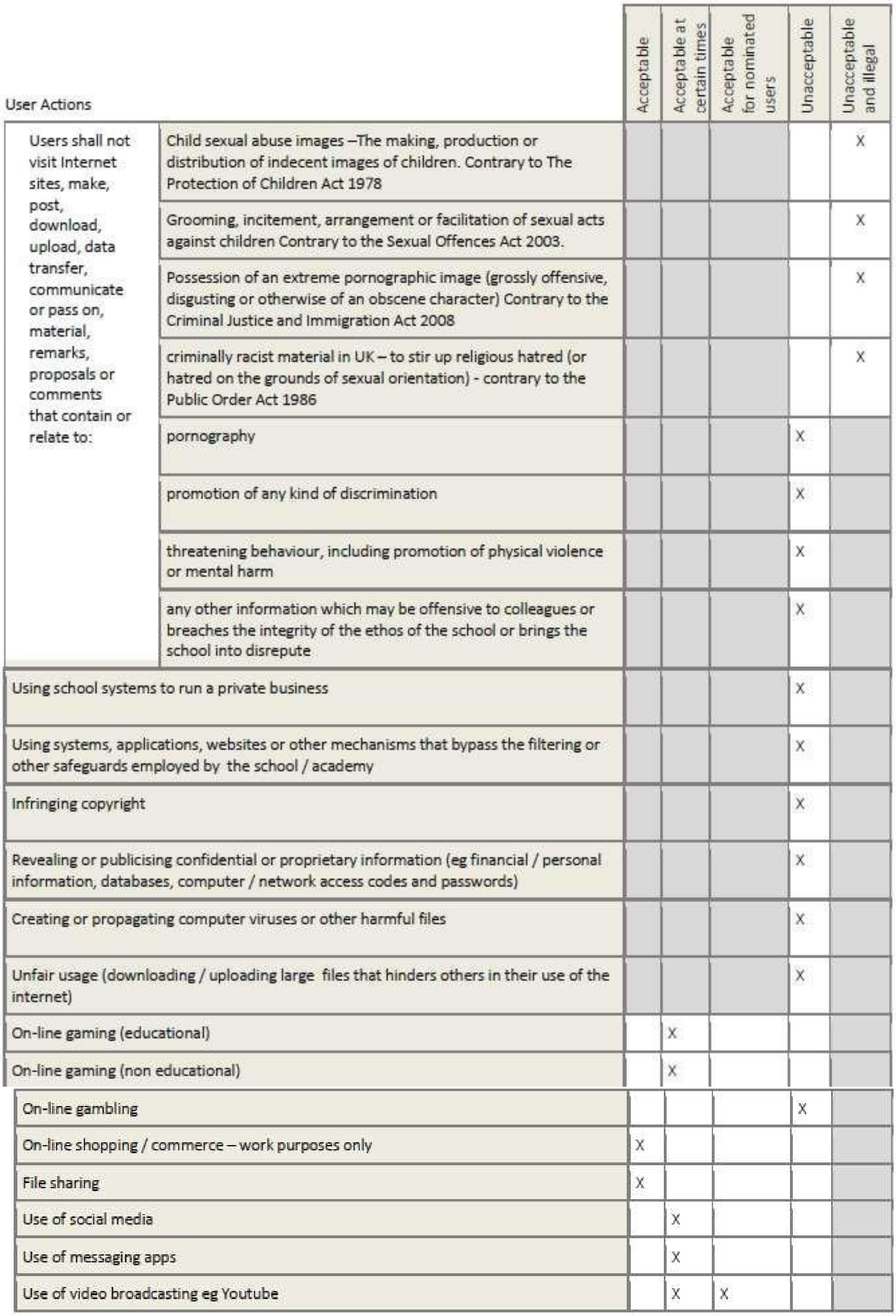
Appendix 2. Key terms in this document:

- Computer Systems – Tablets, laptops, smart watches etc – anything with an input, processing capacity and output
- Cyberbullying - the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature
- Encryption - the process of converting information or data into a code, especially to prevent unauthorized access
- Online safety – preferable to E-safety
- Sexting - send (someone) sexually explicit photographs or messages via mobile phone
- Smoothwall – the school’s internet filtering system
- URL – web site address

Appendix 3. Communications Table

		Staff and other adults					**Students and young people**			
Communication Technologies		Permitted	Permitted at certain times	Permitted for named staff	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones May be brought to school		✓					✓			
Mobile phones used in lessons			✓					✓		
Use of mobile phones in social time		✓								✓
Taking photographs on mobile devices					✓				✓	
Use of tablets and other educational mobile devices		✓					✓			
Use of school email for personal emails					✓					✓
Social use of chat rooms/facilities					✓					✓
Use of social network sites				✓					✓	
Use of educational blogs		✓					✓			

Appendix 4: Inappropriate Activities



User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)			X			
On-line gambling					X	
On-line shopping / commerce – work purposes only		X				
File sharing		X				
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting eg Youtube			X	X		

Appendix 5: Sheffield Safeguarding Hub Online Safety September 2020

Online Safety

Sheffield Children Safeguarding Partnership

Version 14, Sept 20 Safeguarding Sheffield Children website

Safeguarding children & young people online involves a range of issues e.g. cyberbullying, pressure to look ‘right’ & get ‘likes’, fake news, violence, extremist behaviour, grooming, child sexual & criminal exploitation, gambling and sexting.

Cyber-bullying can make children feel scared, upset, isolated & vulnerable, particularly as it can happen whilst alone and/or in their own home.

The main methods of cyber-bullying are:

- Messages, texts, emails, photographs, video’s, sexting, to individuals or groups
- Communicating threats, upset, offense &/or includes racist, sexist, or homophobic content
- Humiliating/abusive phone calls
- Inappropriate communication shared through social networking & gaming sites
- Encouraging other people to bully the victim
- Setting up fake profiles to make fun of someone
- Creating a false identity to send inappropriate communications in someone else’s name
- Using chat rooms & gaming sites to threaten, abuse, lock out, &/or spread rumours
- Send viruses or hacking programs to harvest information or destroy someone’s game/device
- Post intimate, sensitive & personal information without someone’s permission or knowledge

Settings need to educate pupils, parents, carers & staff about the benefits and risks of using this environment and provide safeguards and awareness for users to safely control their online experiences.

Online safeguarding good practice:

- Safe & secure network & broadband connection
- Compliant Information Communication Technology (ICT) security e.g. firewalls, access restrictions
- Up-to-date online-safety policies are understood, implemented & regularly reviewed by staff, pupils, parents & carers
- Staff, pupils, parents/carers responsible ICT use
- Education & training includes progressive & age appropriate online safety curriculum

All settings should have:

- A trained Online-Safety Coordinator who is also a trained Designated Safeguarding Lead/Deputy
- An Online-Safety Policy that reflects your whole-school approach alongside other policies including:
    - Use of cameras, mobile devices, social media
    - Acceptable ICT Use for staff & pupils
    - Pupil and staff behaviour including bullying
    - Online safety & the curriculum
    - Data protection, information sharing & security
    - Filtering and monitoring

The Online-Safety Coordinator is responsible for:

- Undertaking SCSP training
- Safeguarding students online & assessing the needs of students who may be at risk
- Supporting & educating staff, parents & carers

Communication with pupils, staff, parents, carers should include:

- Rules for online safety & internet access in all areas of the setting
- Articles about online-safety in setting newsletters, publicity, website etc.

Pupils, staff, parents, carers should be able to:

- Access & fully understand your age-appropriate Online Safety & Acceptable Use Policies
- Use the internet appropriately & know their use can be monitored & traced to individual users

Assessing & managing risk - settings should:

- Take reasonable precautions to prevent pupil & staff access to inappropriate sites or material
- Maintain an audit of all ICT & social media use
- Teach pupils about responsible & safe use of the internet and what to do when things go wrong
- Ensure staff check sites & links before pupil usage
- Ensure all online platforms used to communicate with pupils & their families (e.g. learning online at home) are fully risk-assessed & monitored
- Ensure all staff & pupils are aware of & can access a clear reporting process for online-safety issues
- Ensure their Acceptable Use & Online Safety Policies considers how all technology, online environments & mobile devices communicate one; access social networks, music, videos & gaming sites; take photographs & record videos
- Carefully manage images & other identifying information about students; obtain their written consent before use; remove/delete image when student has left the setting

An adult may use the above methods to pretend to be someone online to befriend, obtain sensitive information/materials & threaten to expose

It is a crime to:

- Harass or bully via text, email or phone call
- Create, possess, distribute indecent images of child even with consent or if self-generated
- For an adult to have sexual communication with a child under 16 years

The age of criminal responsibility is 10 years.
Head Teachers & staff have powers to search pupils & their possessions, see:

- ‘Reasonable force, searching & screening, Sept 20A’ in **education policies, procedures & guidance**, Safeguarding Sheffield Children website.

Youth gambling:

- 17% of under 16’s gambled online in last 7 days
- Targeted through adverts, apps, influencers, gaming, etc.
- Teach about gambling issues via the curriculum

Useful links:

- Safeguarding Sheffield Children website: Online Safety
- Sheffield Children Safeguarding Partnership Procedures - Online Safety
- UK Safer Internet Centre
- Screening, Searching & Confiscation: advice for schools, DfE 2018

- Safeguarding and remote education
- NSPCC NetAware
- Preventing Bullying, DfE
- NSPCC: Sexting
- Thinkuknow
- YGAM

Other issues:

- Taking a photograph without consent is an invasion of privacy & may be distressing
- Once photos are sent to a device, network or website they are impossible to fully track or delete
- Giving out any personal information (including photos) could put someone at risk of harm
- Location tracking services allow any individual to identify the location of people & devices

3 key concerns when using the internet:

- **Content** – harmful material or ideas e.g. racist, pornographic, bullying, sexual, homophobic
- **Contact** – who interacting with online, are they encouraging student to do something harmful?
- **Conduct** –online behaviour e.g. making, sending, receiving explicit images, bullying, gambling

Most issues can be resolved through regular education and targeted training.

Consider whether the student was:

- Posting inappropriately on the internet?
- Offered e.g. gifts or money for something?
- Meeting someone through the internet?
- Supervised whilst using the internet?
- Supported/protected by parents/carers?
- Being shown harmful material?
- Able to understand & give reasons for risk-taking?
- At risk of or suffering significant harm?

Top tips:

- **Never publicise 'unsafe' sites**: it encourages people to look & implies other sites are 'safe'
- Teach staff, students, parents & carers to act safely in all internet use
- If your concern is low level, discuss with parents or carers & agree a plan
- Where appropriate, assess child and families needs with an FCAF

If any child or young person is at risk of significant harm refer them immediately to The Sheffield Safeguarding Hub, tel. 0114 2734855 or to their current social worker

If you think parents/carers are part of the risk or if a crime may have been committed, **do not inform them before** you discuss with The Hub

Ensure other involved practitioners are aware of your online safety concerns and incorporate this into the support they are providing

Online Safety

Version 14, Sept 20 Safeguarding Sheffield Children website

Assessing risks and problems Child or young person's level of need:

Universal

- Has a range of IT skills and understands how the internet works and its global audience
- Safely enjoys the benefits of the internet and is able to communicate safely with friends and family
- Maintains personal security when using chat rooms, gaming etc.
- Does not disclose personal details of friends to unknown parties
- Family aware of use and understand safe use principles
- Child shares interest with parents

Universal plus/partnership plus

- Some IT skills but doesn't really understand how the internet works
- Uses the internet carelessly, visiting unregulated sites
- Visits adult sites and views explicitly sexual or violent material
- Is the victim or perpetrator of occasional low level cyber-bullying
- Has IT skills but using them to access unsuitable areas of the internet
- Uses the internet to establish contact with unknown others and discloses contact details
- Transmits pictures/video of self or others which could be used by internet predator or for cyber bullying
- Discloses address and phone details
- Agrees to meet stranger with peer(s)

Targeted/acute/specialist

- Visits illegal sites or sites designed for adults and develops an interest which may lead to criminal or exploitative actions
- Exposes friends to risk by disclosing details to strangers
- Posts explicitly sexual/ violent material including photos/ video of self or others
- Discloses stranger abuse resulting from internet contact
- Is the victim or perpetrator of sustained and/or serious cyber-bullying that includes disclosure of personal and identifying information
- Agrees to meet stranger alone

Action from practitioners:

- Child is benefiting from parental guidance and curriculum activity
- Continue discussion about online safety in curriculum

- Parents, carers and school provide advice and consider steps which need to be taken
- Parents and carers are given advice as needed
- Age appropriate access controls put in place
- Discuss with DSL/D in school
- Consider action plan

- Inform DSL/D
- Notify police
- Inform parents/carers if safe to do so
- Notify other parents/carers if appropriate

All pupils/students should be taught to evaluate the content of online information, e.g.:

- Are representations of body image photo-shopped or air-brushed?
- How other people portray their lives online
- How to spot fake news
- How to disengage and control their internet use