Online Safety Policy

Reviewed: March 2024

Next Review: March 2027

Signed:

Introduction

Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour and develop effective strategies for staying safe and making a positive contribution online. Taken from Education for a Connected World – 2020 edition.

Currently the internet technologies children and young people are using both inside and outside of the classroom may include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile devices with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web- based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Cardinal Road Infant and Nursery School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The resources used by pupils in school are carefully chosen by the teachers and determined by curriculum policies. Use of the Internet, by its nature, might provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times, they may be able to move beyond these, to sites unfamiliar to the teacher.

There is cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet.
- Describe how these fit into the wider context of our discipline and PSHE policies.

- Demonstrate the methods used to protect the children from sites that have unsuitable content.

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

We feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Whole School Approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-safety education programme for pupils, staff and parents.

'Keeping Children Safe in Education' obliges schools in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

Roles and responsibilities

All teachers are responsible for:

- promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. All staff should be familiar with the school's policy
- the safe use of e-mail
- the safe use of the Internet
- the safe use of the school network, equipment and data
- the safe use of digital images and digital technologies, such as mobile devices and digital cameras
- the publication of pupil information/photographs on the school website
- the procedures in the event of misuse of technology by any member of the school community in providing e-safety education for pupils.

Staff are updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction (see appendix for staff acceptable use agreement).

The SLT together with a member of the governing body are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of our provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Managing the school e-safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- E-safety information is be prominently displayed.

E-safety in the curriculum

ICT and online resources are increasingly used across the curriculum. E- safety guidance is to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

- We provide opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that might be encountered outside school is done when appropriate and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the computing curriculum.
- Pupils are made aware of the impact of online bullying (including through PSHE) and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
- Pupils are taught to critically evaluate materials and learn effective searching skills through cross curricular teacher models, discussions and via the computing curriculum

- Pupils are taught the importance of maintaining good manners and respect when communicating with others on line.

Introducing the e-safety policy to pupils

- E-safety rules are posted in all networked rooms and discussed with pupils at the start of each year
- Pupils are informed that network and Internet use will be monitored.
- E-safety are included more prominently in both the PSHE and computing curricula.
- E-safety has a high profile and is covered every time pupils use an internet enabled device.

Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- Students have supervised access to Internet resources through the school's internet technology.
- Staff preview any recommended sites before use.
- Staff should do all they can to prevent adverts playing to children when playing videos online. The content of adverts can be unpredictable and unsuitable. If this is unavoidable, they are monitored and skipped when possible and discussions are taken place around the purpose of adverts.
- Raw image searches are discouraged when working with pupils. When they are made, they are monitored carefully.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- Our internet access is controlled through Hounslow LA's web filtering service.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- Pupils are taught to communicate in a kind way at all times including on electronic devices.
- Pupils are taught to turn their screen off and to tell the nearest adult if they discover unsuitable content on their device.
- Staff should make sure their email is not visible to the children e.g. on the interactive board or monitor.

- It is the responsibility of the SLT and governors and by delegation to the network manager, to ensure that anti- virus protection is installed and kept up-to-date on all school machines.

Mobile devices (iPads)

We recognise that mobile devices (such as iPad) provide instant access to the internet through both 'apps' and browsing the web. They have a vast range of educational opportunities but it is also important to ensure that they are used appropriately and that children are aware that they are open to the same dangers as using the internet on a computer. These dangers include having advert banners which take the user out of the app to a web page. Apps installed on iPads are carefully considered for their educational value and when possible, versions without adverts are installed. Internet access on mobile devices will be through the schools wireless system which is also filtered by the LA internet provider. Members of staff must ensure children are aware of expectations and appropriateness when using mobile devices. Staff need to be aware that mobile devices are harder to see from afar and there is the potential for children to easily hide from view things on their screen (whether intentionally or not).

E-mail

The use of email within school is an essential means of communication for staff and parents. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age.

- Pupils are introduced to email as part of the computing Scheme of Work.
- The school gives staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- Staff must protect confidential documents with passwords or send using extra levels of security e.g. send using 'egress'.
- Staff are not to use pupils' full names in emails.
- Staff sending emails to an external group should protect email addresses as appropriate using BCC or should send emails individually.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:

- on the school web site
- in printed publications that the school may produce for promotional purposes
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Pupils' names will not be published alongside their image and vice versa without permission from the parents. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting pupils' work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Social networking and personal publishing

We block/filter access for pupils to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Video Conferencing

The use of web cams and video conferencing is becoming more common in schools.

- If using video conferencing to conduct parent / carer meetings involving the parents / carers of more than one family, it must be made clear that no confidential information will be discussed during the meeting.
- All pupils must be supervised by a member of staff when video conferencing.
- If video conferencing is used to communicate with parents / carers or pupils, professional conduct must be maintained, the professional standards upheld and the safeguarding policy followed.
- Staff should state clearly if the call is being recorded.

The school website and home learning

A website can celebrate good work, promote the school, and publish resources for projects and research, and link to other good sites of interest.

- Home information and e-mail identities will not be included, only the point of contact to the school i.e. phone number, school address and e-mail
- Work displayed will be of the highest quality and reflect the status of the school
- With parental consent, photographs of children participating in school activities and named work will be presented
- All homelearning worksheets etc must be checked for their content and suitability prior to being uploaded onto the school's website.

- All links to external sites needs to be checked for their content and suitability prior to being added to the school's website.

Home learning on the online platform (Microsoft Teams)

When using Teams for home learning:

- Permissions should be set to ensure pupils do not have the ability to communicate in chat to each other.
- Permissions should be set to ensure pupils do not have the ability to record video calls.
- Staff must ensure content they submit and approve is safe for others to view and considers the safeguarding of the pupils. Staff for example, check the background of photos and videos and the audio.
- General information and feedback can be given using Teams but sensitive information should not be discussed with parents using Teams in a channel. Other users in the channel would be able to view the messages. Even if there is only one person in the channel, if other people are added to that channel at a later date, they would be able to see all messages in that channel or team.
- Remember, messages (posts and replies) in channels are visible by all in that channel.
- Staff are to regularly review posts in their teams to ensure all posts are appropriate.
- If inappropriate messages are posted, they must be deleted. If someone continues posting inappropriate content, they are to be muted.
- If live sessions are held with pupils, a second member of staff should be signed in as an observer to monitor the session.

Online learning journals

Online learning journals are used to record pupil progress and to communicate with parents and staff. Observations including photos and videos are uploaded along with comments by staff. Parents / carers who have access are also able to upload observations including photos, videos and comments. Once observations have been approved by staff, users can then leave comments and 'like' observations.

- Ensure parents / carers consent to other users e.g. uncle having access to the online journal.
- Staff must check content uploaded by parents / carers before approving the post.
- Staff must ensure content they submit and approve is safe for others to view and considers the safeguarding of the pupils. Staff for example, check the background of photos and videos and the audio.
- Whilst it is made clear that other pupils will be in photos and videos, efforts will be made to ensure that this is kept to what is necessary.

Mobile Phones and smart watches

The pupils do not bring mobile phones or smart watches to school. They are too young for this responsibility. If a mobile phone or smart watch were to be brought into school it would be stored in the office and given to the parent/carer at the end of the school day.
Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. If staff need to take photos, they must be taken on a school device, not their own personal mobile or iPad etc. Staff are not to use their phones around the pupils.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Searching

Staff may lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Any data, files or images that are believed to be illegal must be passed to the police as soon as practicable, including pornographic images of children, without deleting them.

Any data, files or images that are not believed to be unlawful, may be deleted or kept as evidence of a breach of the school's behaviour policy.

Data protection

Members of staff are made aware of the importance of data protection. They are issued with an individual password to access information on the servers and advised to save confidential information in their secure folders on the system so that it is kept private. They can also be

issued with encrypted USB memory sticks to ensure that data is secure when transporting. Staff only have access to electronic systems required to perform their role.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the internet, deliberately to upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it.

Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about cyberbullying as part of our computing curriculum. They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- Know who they can speak to re any problems with cyberbullying.

The school will not tolerate cyber bullying and pupils must let an adult know if they receive an inappropriate message. Measures are put into place to prevent this from happening but no system is fool proof.

Introducing staff to the e-safety policy

- All staff will be given the e-safety policy and its application and importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on our e-safety policy will be provided as required.

Expectations of Pupils using the Internet

- We expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access and language they use.
- Pupils using the internet are expected to not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to turn the screen off and report it immediately to a member of staff. Staff should use their own discretion on reporting it to the ICT coordinator so that the Service Provider can block further access to the site.

- Pupils are expected to use kind and inoffensive language in their communications and contact only people they know or those the teacher has approved. They have been taught the rules of etiquette in e-mail and are expected to follow them.
- Pupils must have or ask permission before accessing the Internet and have a clear idea why they are using it.
- Pupils should not deliberately access other people's files unless permission has been given.
- Computers should only be used for schoolwork and research unless permission has been granted otherwise.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made, this will be taught and reinforced every year.
- Pictures or work should not be brought into school on CD ROM or memory stick. The use of external memory sources is not allowed because of the potential of viruses and at the advice of our data protection advisors (see our GDPR policies). Work from home could be uploaded to our secure platforms e.g. Tapestry or emailed, or printed.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

APPENDIX I

Acceptable Use of ICT Agreement
Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

All staff members are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with ICT coordinator or Head teacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Board in teaching and learning time.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with parents and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on Pupil Asset) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely for an authorised purpose.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies including social media can be monitored and logged and can be made available, on request by the Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I understand I should keep my personal views to myself when posting on social media and that I should consider how the things I 'like' reflect my views.
- I will not post anything negative on social media about the children, staff and school.
- I understand that it is strongly recommended that I do not write about the children, staff and school in closed, 'private' messaging services outside the school's communication tools and that doing so may lead to consequences.
- I will support and promote the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use my own, personal mobile phone (or similar device) around the children.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school
Signature …… Date ……
Full Name ……

APPENDIX II

Online Resilience Tool (headstartkernow.org.uk)

Devices

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Being left with a tablet/smartphone unsupervised for 30 minutes or more	Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Ownership of their own devices	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Preoccupation with digital devices	Potentially Harmful	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful
Being left alone with a device with parental controls in place for up to 10 minutes	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Interacting with a digital device	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Upset or aggressive response to withdrawal of device (beyond what is normal for the child)	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Knowing passwords to parental devices	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Bypassing parental controls	Harmful	Harmful	Potentially Harmful	Not Harmful	Not Harmful
Reaching for a device as soon as they wake up	Potentially Harmful	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful
Using screens less than an hour before bedtime	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Use of digital devices after bedtime	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful

Education

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Learning how devices work	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Learning how to write code with supervision	Not applicable	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Learning how to write software	Not applicable	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Doing homework alone	Not applicable	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Supervised schoolwork using online technology	Not applicable	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Accessing pro-self-harm or pro-ana (pro-anorexia) sites	Harmful	Harmful	Harmful	Harmful	Harmful
Using unreliable sites to find out about personal issues	Harmful	Harmful	Harmful	Harmful	Harmful
Using reliable sources to find out about personal issues (Brook, Talk to Frank, NHS direct)	Not applicable	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Searching for information on losing weight	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Researching issues in an unsupported way e.g. self-harm/ depression, eating disorders	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Guided research/learning	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Writing a blog	Not applicable	Potentially Harmful	Potentially Harmful	Potentially Harmful	Not Harmful
Accessing 'deep web' sites using browsers such as Tor to explore what is there	Not applicable	Not applicable	Potentially Harmful	Potentially Harmful	Potentially Harmful
Learning about online issues and discussing their opinions	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful

Extremism

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Accessing extremist/pro-self-harm/ suicide social media accounts as part of ongoing recovery or offering support	Not applicable	Harmful	Harmful	Harmful	Harmful
Radicalisation (this could be through specific extremist sites or through seemingly innocent forums such as those attached to games)	Harmful	Harmful	Harmful	Harmful	Harmful
Persistently viewing extremist sites	Harmful	Harmful	Harmful	Harmful	Harmful
Accessing pro-self-harm/suicide sites	Not applicable	Harmful	Harmful	Harmful	Harmful
Repeating extremist views read about online	Not applicable	Harmful	Harmful	Harmful	Harmful
Accessing extremist websites	Not applicable	Harmful	Harmful	Harmful	Harmful

Friends and family

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Group messaging and opting to leave or mute a group chat	Not applicable	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
One to one messaging	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Showing someone distressing videos they don't want to see	Harmful	Harmful	Harmful	Harmful	Harmful
Meeting online friends unsupervised	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Meeting online friends if have skyped/facetimed (whilst taking appropriate precautions)	Harmful	Harmful	Harmful	Potentially Harmful	Not Harmful
Meeting online friends as part of a group.	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Meeting online friends with supervision (eg a parent or carer is present)	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Sharing things seen online with friends in person	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Watching films/TV with family member	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Supervised Skyping with remote family members	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Curiosity around digital devices	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
A variety of interactions and responses to devices	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Being aware of/being told there is 'adult content' online.	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Talking about how they feel if they see something upsetting	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Interest/involvement in family social media e.g. looking at news feed, asking to see pictures	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful

Friends and Family - Continued

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Secretive* use of online device	Not applicable	Potentially Harmful	Potentially Harmful	Potentially Harmful	Not Harmful
Mimicking online behaviour	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Not Harmful
Ganging up on or isolating others online	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Contact with strangers online	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Excessively sharing personal information online	Not applicable	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Watching adult content	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Not Harmful
Online shopping with own money	Harmful	Harmful	Potentially Harmful	Not Harmful	Not Harmful
Online shopping with parents/ carers' money without their knowledge	Harmful	Harmful	Harmful	Harmful	Harmful
Asking for help to block or report something	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Not reporting upsetting or harmful content	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Repeated conflict about rules	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful

Gaming

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Disrupted sleep through device dependence/gaming	Harmful	Harmful	Harmful	Harmful	Harmful
Online gambling	Harmful	Harmful	Harmful	Harmful	Potentially Harmful
Receiving gifts in online games from family members	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Receiving gifts in online games from strangers (someone unknown to parents)	Harmful	Harmful	Harmful	Harmful	Potentially Harmful
Gaming alone	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Playing age-appropriate games with a family member	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Watching a family member play age-appropriate games	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Age-appropriate gaming with adult supervision	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Playing age-restricted games unsupervised	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Not Harmful
Playing age restricted games with direct parental supervision	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Filming themselves/friends playing age-appropriate games	Not applicable	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Gaming (on or offline) in line with age restrictions	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Age appropriate multiplayer online gaming	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Not Harmful
Playing ads for offer of rewards	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Prolonged period of upset or anger after gaming	Harmful	Harmful	Harmful	Harmful	Harmful

Relationships and Sex

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Setting up a fake social media account to explore gender identity or sexuality	Not applicable	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Taking and sending/receiving nudes/sexting for any reason	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Accidentally receiving nudes	Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Sexualised posing online	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Sexual webcamming	Harmful	Harmful	Harmful	Harmful	Harmful
Selling nudes	Harmful	Harmful	Harmful	Harmful	Harmful
Retention of indecent images of peers	Harmful	Harmful	Harmful	Harmful	Harmful
Forwarding nudes of other young people, including friends, without consent	Harmful	Harmful	Harmful	Harmful	Harmful
Pressuring someone to send nudes/ sext	Harmful	Harmful	Harmful	Harmful	Harmful
Coercive behaviour toward others using digital technology (for example tracking others, accessing other people's accounts)	Harmful	Harmful	Harmful	Harmful	Harmful
Accessing dark web** to engage with services (for example buying drugs online, downloading extreme pornography)	Harmful	Harmful	Harmful	Harmful	Harmful
Frequent access to pornography	Harmful	Harmful	Harmful	Potentially Harmful	Not Harmful
Accessing pornography as a one off	Harmful	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful
Watching violent/extreme pornography	Harmful	Harmful	Harmful	Harmful	Harmful

Relationships and Sex - Continued

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Compulsive*** use of pornography	Harmful	Harmful	Harmful	Harmful	Harmful
Finding out about sexual behaviours using pornography	Harmful	Harmful	Harmful	Potentially Harmful	Not Harmful
Excessively watching pornography	Harmful	Harmful	Harmful	Harmful	Potentially Harmful
Looking at images of different body types/genital types to understand range of normal	Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Accidental access of sexual content	Harmful	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful
Online dating with adults	Harmful	Harmful	Harmful	Harmful	Potentially Harmful
Online dating with peers	Not applicable	Not applicable	Harmful	Potentially Harmful	Potentially Harmful
Online dating with peers (whilst taking appropriate precautions)	Not applicable	Not applicable	Harmful	Potentially Harmful	Not Harmful
Sharing indecent or distressing images with peers	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Sexual or violent language	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Role-playing or parroting adult content (e.g. sex/violence)	Harmful	Harmful	Potentially Harmful	Not Harmful	Not Harmful
Catfishing/direct messaging someone pretending to be someone else	Not applicable	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Not blocking someone who has been nasty to you online	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Tracking friends through location sharing	Not applicable	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Looking at partners phone with consent	Not applicable	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful

Socail media

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Having celebrity role models, aspiring to be like a celebrity	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Playing with filters	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Using filters on pictures	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Excessive posing in selfies	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Obsession with selfies	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Requesting images to be airbrushed	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Taking but not sending selfies	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Accidentally sending selfies	Potentially Harmful	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful
Placing oneself at physical risk in order to take selfies or generate online content	Harmful	Harmful	Harmful	Harmful	Harmful
Asking to have a photo removed/ not put on social media	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Refusing to remove a picture of someone else when asked	Harmful	Harmful	Harmful	Harmful	Harmful
Removing a picture of someone else when asked	Not applicable	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Regular social media use	Harmful	Harmful	Potentially Harmful	Not Harmful	Not Harmful
Compulsive** use of social media including checking during the night	Harmful	Harmful	Harmful	Harmful	Potentially Harmful
Being secretive* about direct messages	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Fear of missing out leading to separation anxiety from social media	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Anxiety around digital communications	Harmful	Harmful	Harmful	Potentially Harmful	Potentially Harmful
Feeling anxious because messages have not been answered	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Messaging friends on shared devices	Not applicable	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Sending friends direct messages	Not applicable	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Having their own private social media account	Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Having a public social media account	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Not Harmful
Using fake social media accounts to trick or humiliate others	Harmful	Harmful	Harmful	Harmful	Harmful
Making content and publishing/ posting on online	Not applicable	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Running Snapchat streaks with friends	Not applicable	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Instagram/Snapchat stories	Not applicable	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Sharing images with peers with parent/guardian oversight	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Blocking and reporting someone for posting inappropriate content	Not applicable	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Looking at social media with friends/family	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Commenting on a status	Not applicable	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Sharing social media/device passwords with others	Not applicable	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Private use of digital platforms	Harmful	Harmful	Potentially Harmful	Not Harmful	Not Harmful

Social Media - Continued

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Use of digital platforms without parents/carers knowledge	Harmful	Harmful	Potentially Harmful	Not Harmful	Not Harmful
Having a YouTube channel	Harmful	Harmful	Potentially Harmful	Not Harmful	Not Harmful
Becoming an influencer/brand ambassador	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Talking about high numbers of subscribers/followers on online cast/social media channel (for example YouTube/Instagram).	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Actively promoting social media or YouTube channel among peers	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Not Harmful
Online interaction with strangers	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Seeing pornographic content on social media	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Not Harmful
Being concerned about parental or institutional monitoring	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Curating feed on social media	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful

Watching Content

Behaviour	0-5 years	6-8 years	9-12 years	13-15 years	16-18 years
Being obsessed with celebrities, wanting to be a specific celebrity	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful
Accessing illegal content	Harmful	Harmful	Harmful	Harmful	Harmful
Watching age-appropriate digital content with friends unsupervised	Harmful	Potentially Harmful	Not Harmful	Not Harmful	Not Harmful
Role modelling age-appropriate characters	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Watching online content on a device with parental controls	Not Harmful	Not Harmful	Not Harmful	Not Harmful	Not Harmful
Watching films/TV online alone	Harmful	Potentially Harmful	Potentially Harmful	Not Harmful	Not Harmful
Not being able to sleep after seeing scary or upsetting content online	Harmful	Harmful	Potentially Harmful	Potentially Harmful	Potentially Harmful