



Queen
Elizabeth
School

Online Safety Policy

Effective from: *September 2024*

Signed by:

Reviewed: 20 October 2024

Next review date: *September 2025*

1. Rationale

The requirement to ensure that children and young people can use the internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Un-authorized access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others including strangers.
- Cyber-bullying
- Access to unsuitable video / internet games
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other policies including those for ICT / behaviour / anti-bullying / child protection.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- o Human Rights Act 1998
- o The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- o Education Act 2011
- o Freedom of Information Act 2000
- o Education and Inspections Act 2006
- o Keeping Children Safe in Education 2023
- o Searching, screening and confiscation: advice for schools 2022
- o National Cyber Security Centre (NCSC): Cyber Security for Schools
- o Education and Training (Welfare of Children) Act 2021
- o UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- o Meeting digital and technology standards in schools and colleges

2. Purpose

This policy is designed and intended to reinforce the Acceptable use policies for Staff and Volunteers, Pupils, Parents/Carer's and provide guidelines and working practices for the effective and safe use of the internet, email and other communications technologies in the school, which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

3. Unacceptable use examples

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams

- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

4. Scope of the Policy

New technologies have become integral to the lives of children and young people today, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity, and increase awareness of context to promote effective learning. Children and young people should always have an entitlement to safe internet access.

The requirement to ensure that children and young people can 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.

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school and should help to ensure safe and appropriate

use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students/pupils themselves. These responsibilities are reflected in the Acceptable Use Policies for pupils, staff and volunteers and parents/carers.

5. Development and Monitoring

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

As part of this policy, all online activity will be monitored by **Smoothwall**. All incidences will be reported to the head teacher or designated safeguard lead and pupils and any incidents will be treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.

The school will monitor the impact of the policy using:

- Smoothwall Incident reports
- Feedback from staff, pupils, parents / carers, governors
- Logs of reported incidents
- Internet activity monitoring logs

6. Roles and Responsibilities

Governors:

Governors are responsible for the approval of the e-safety policy and for reviewing its effectiveness.

Headteacher and Senior Management:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, through the day-to-day responsibility for online safety will be delegated to the Computing subject co-ordinator and Designated Safeguarding Lead.
- The Headteacher and Designated safeguarding lead will action incidences shared by Smoothwall monitoring.

- The Headteacher is responsible for the implementation and effectiveness of this policy. She is also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement
- The Headteacher / Senior Management are responsible for ensuring that the Computing Subject Co-ordinator / Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles
- The Headteacher and another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (refer to Managing Allegations against a member of staff guidance)

Computing Subject Leader and Designated Safeguarding Lead (DSL) and Deputy DSLs:

- Takes day to day responsibility for Online-safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Reports to the School Management Team serious breaches of the online safety policy.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Coordinate teaching and training responses following online safety incidences.
- Are trained in and shares with staff an awareness and understanding of online safety issues and the potential for serious child protection issues that can arise from:
 - Sharing of personal data
 - Access to illegal / inappropriate materials
 - Inappropriate on-line contact with adults / strangers
 - Potential or actual incidents or grooming
 - Cyber-bullying
 - Sexting
 - Revenge pornography
 - Radicalisation (extreme views)
 - CSE

The Network Manager and Computing Subject Leader are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the online safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
- The school's filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- Coordinating with **Trident IT support** who provide all filtering.
- That they keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- That the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the School Business Manager/ Headteacher for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

- They have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood the e-safety policy, school Acceptable Use policy.
- They report and suspected misuse or problems to the Computing Subject Leader / Designated Safeguarding Lead of Deputy DSLs for investigation / action / sanction.
- Digital communications with pupils and parents / carers (email/voice) should be on a professional level.
- Students / pupils understand and follow, as appropriate for age and ability, the school's online safety and acceptable use policy.
- Students / pupils understand and follow e-safety rules and they know that if these are not adhered to, sanctions will be implemented in line with our behaviour and anti-bullying policies.
- In lessons where internet use is planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

- Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to agree to before being given access to school systems. (nb. For some pupils it would be expected that parents/ carers would sign on behalf of the pupils)
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's e-safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these

issues through parents' evenings, newsletters, letters, website / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Policy
- Accessing the school website / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Parents/carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

7. Education and Training

Education – Pupils

E-safety education will be provided in the following ways, as appropriate to pupils' age and ability:

- A planned online safety programme should be provided as part of Computing / PSHE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key online safety messages should be reinforced as part of planned programme of assemblies and tutorial / pastoral activities.
- Students / pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile device both within and outside school.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students / pupils are taught the importance of keeping information such as their password safe and secure
- Rules for the use of ICT systems / internet will be made available for pupils to read.
- Staff should act as good role models in their use of ICT, the internet, and mobile devices.
- Students / pupils are taught how to keep safe through effective / good online-safety practice as part of an integral elements of the school Computing curriculum and within their ICT learning.
- Where students / pupils are allowed to freely search the intranet, e.g. using search engines, 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, students 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 Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents and Carers

Many parents and carers have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-lines experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. **“There is a generational digital divide”.** (Byron Report)

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, web site
- Parents evenings
- Reference to external online safety websites
- High profile events such as Internet safety day
- Family learning opportunities
- In addition parents can access online safety guides through the school newsletter and in **Appendix 1** (a sample set)

Education and Training -Staff

It is essential that all staff receive online-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online-safety training will be made available to staff. An audit of the online-safety training needs of all staff will be carried out regularly.
- All new staff should receive online-safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school e-safety policy and Acceptable Use Policies.
- The Computing Subject Co-ordinator (or other nominated person) will provide advice / guidance / training to individuals as required.
- No staff will accept a friend request from pupils on social media.

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there

8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

8. Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence?

Before a search, the authorised staff member will:

- Assess how urgent the search is and consider the risk to other pupils and staff.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation.

Authorised staff members may examine, and in exceptional circumstances erase, any data, or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening, and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

9. Technical – Infrastructure / equipment, filtering, and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed through the managed service provider, in ways that ensure that the school meets the online-safety technical requirement for West Sussex Local Authority
- Servers, wireless systems, and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- Staff will be made responsible for the security of their username and password, must not allow other users to access the system using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by service provider. Any incidents or activities regarding filtering will be handled in accordance with WSSfS.
- Remote management tools are used by the managed service provider to control workstations and view users' activity.
- Appropriate security measures are in place, provided by the managed service provider, to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Guest can access the school network using the guest login, guests will not give access to personal information about pupils or staff.
- The school infrastructure and individual workstations are protected by up-to-date anti-virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the school Personal Data Policy

10. Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to 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 are carefully selected and comply with good practice 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or social media.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

11. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on [digital and technology standards in schools and colleges](#), including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

12. Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Pupils should therefore not use other email systems when in school, or on school systems.
- Users need to be aware that email communications may be monitored.

- Users must immediately report, to the Designated Safeguarding Lead – the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers must be professional in tone and content and be via official used systems.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include an unsuitable or abusive material.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer.

13. Unsuitable / inappropriate activities

QEII School believes that the activities listed below would be inappropriate in a school context and those users, should not engage in these activities in school or outside school when using school equipment or systems. 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
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity,
- Computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in U
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm 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.
- Using school systems to run a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Local Authority and / or the school.
- Uploading, downloading, or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial /personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files

- Carrying out sustained or instantaneous high volume network traffic (downloading /uploading files) that causes network congestion and hinders others in their use of the internet.
- On-line gambling
- On-line shopping / commerce
- File sharing.
- Use of social networking sites
- Use of video broadcasting e.g. YouTube (for personal use)

For further information, please refer to Full and Summary Guidance for the Safer Use of the Internet by Staff Working with Young People.

14. 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 by pupils, staff or any other user 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 incident should be following in accordance with the safeguarding policy and is necessary, the police should also be informed.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

15. Monitoring and review

This policy will be reviewed annually, or earlier if necessary, in line with national and/or local updates.

Appendix 1 Online safety guides




National Online Safety
#WakeUpWednesday

12 Social Media Online Safety Tips

FOR CHILDREN WITH NEW DEVICES

With Christmas only a few weeks away, many of you will be using social media to share your excitement with friends and family. Being active on social media is a great way to show others how much fun you're having, but it's important that you know how to use these apps safely and securely so that bad things don't happen. By following our safety tips below, you can make sure that your personal information stays private, your postings are positive and that your social media use overall is responsible, healthy and most of all enjoyable.

- 1 DON'T ACCEPT FRIEND REQUESTS FROM STRANGERS**




Make sure that you set your profile to private so that people you don't know can't find you online. Always tell a trusted adult if a stranger or somebody you don't know sends you a message or a friend request.
- 2 NEVER SHARE YOUR PERSONAL INFORMATION WITH PEOPLE YOU DON'T KNOW**

Keep your personal information personal. Sometime people online aren't always who they say they are and might ask you to share things that you don't feel comfortable sharing.
- 3 DON'T SHARE EMBARRASSING PHOTOS OR VIDEOS OF OTHERS ONLINE**




This could really upset them and could get you into a lot of trouble. Always think twice before posting anything on social media and treat people online as you would in real-life.
- 4 NEVER SEND NAKED PICTURES OF YOURSELF TO OTHERS**

This is illegal if you are under 18 and you could get into trouble with the Police. If you are being pressured by someone, always say no and tell a trusted adult. Even if you think it is innocent fun, the photo could be shared with other people and you won't be able to control who else sees it.
- 5 CREATE A POSITIVE ONLINE REPUTATION**




Always be kind and polite when posting comments on social media and only upload pictures and videos of things you are proud of. This forms part of your digital footprint. Everything you do online can be tracked and monitored and could affect what people think of you in real-life if it is negative.
- 6 LIMIT YOUR SCREEN TIME**



Social media can be addictive, and it is easy to keep checking newsfeeds or your notifications every 5 minutes which can affect your behaviour and stop you from doing other things. Remember to only use your phone at certain times of the day, turn notifications off at bedtime and go out and have as fun as much as possible. This will keep you fit and healthy and make you appreciate there's more to life than just what's on social media.
- 7 BLOCK ONLINE BULLIES**


Sometimes people might say nasty things to you online or post offensive comments on your pictures or videos. If this happens, always tell a trusted adult who will help you block them from your profile and support you in taking further action.
- 8 REPORT INAPPROPRIATE CONTENT**




If you see something on social media that you don't like, offends you or upsets you, you should always report it to a trusted adult. You should also report it to the social media app who will be able to remove the content if it is against their user policy and can block the person who posted it.
- 9 ONLY USE APPS WHICH YOU ARE OLD ENOUGH TO USE**




Before downloading any new social media app, always check the age-rating. If you need help, ask your parent or carer to make sure that the app is safe for you to use and never download anything which you are too young for as it may contain content that isn't safe for you to see.
- 10 ALWAYS SECURE ALL YOUR SOCIAL MEDIA PROFILES WITH A PASSWORD**




This will help to keep your private information safe and won't allow others to access your profiles without your permission. Make sure your passwords are memorable and personal to you but something which other people can't guess, and always share them with your parents just in case you forget them.
- 11 ASK PARENTS TO SET-UP 'PARENTAL CONTROLS' FOR SOCIAL MEDIA**



When you download a social media app, you should always ask a trusted adult to help you set it up for the first time. This will help you control who sees what you post, who can contact you and make sure you are able to enjoy using the app safely and securely.
- 12 ALWAYS TALK TO YOUR TRUSTED ADULT IF SOCIAL MEDIA IS MAKING YOU UNHAPPY**



Sometimes, social media can make us feel bad about ourselves or sad that we aren't the same as someone else or doing the same things as someone else. Remember, if you ever feel this way, it's really important to talk to your trusted adult(s) like your parents, carers, other adult family members or a teacher, all of whom will be able to support you and discuss your feelings with you to help make you feel better.



www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety

STAY SAFE ON NEW DEVICES

Whether you're an internet newbie or a pro at surfing the web, it's always important to keep online safety in mind. We've pulled together a list of top tips to make it easier for you to protect yourself and your devices in the digital world – helping you steer clear of hazards like misleading information and vicious viruses. There's never a bad time to refresh your internet safety knowledge, but it's an especially smart thing to do before you start using any shiny new devices!



www.nationalonlinesafety.com



[@natonlinesafety](https://twitter.com/natonlinesafety)



[/NationalOnlineSafety](https://www.facebook.com/NationalOnlineSafety)



[@nationalonlinesafety](https://www.instagram.com/nationalonlinesafety)

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 04.01.2023

SPOTTING ADS ON SOCIAL MEDIA

Do you always know when you're seeing an ad on your social media feed? You might not! Some ads look just like any other post - they might be funny or cool, but really they're trying to sell you something without you realising. But here are some ideas for spotting ads like a pro!

Look closely at the profile picture

Pay attention to the account name

Check if it says "sponsored" f @ or "promoted" 🐦

A 'verified' tick can still mean it's an ad

Be savvy with high numbers of likes and shares

Study the hashtags for clues about the post's purpose



NOS National Online Safety®
#WakeUpWednesday

At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it's needed. This guide focuses on one of many issues which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know about LIVE STREAMING

Live streaming involves broadcasting and watching videos online in real time, often on social media or via platforms like YouTube and Twitch. Viewers can interact through comments, chats and reactions during the broadcast: such instant engagement makes this an exciting way to share experiences, learn from others and build digital communities. Despite the many positives, live streaming also creates a potential platform for unsuitable content and poses some risks to children: it's essential to keep privacy and safety in mind and comply with each site or app's age restrictions.

AGE RESTRICTION

13+
16+ 18+

Age varies by platform

WHAT ARE THE RISKS?

LACK OF AGE VERIFICATION

Despite their age restrictions, some platforms don't require proof of age at sign up – meaning that anyone can register for an account (and potentially pretend to be older or younger than they actually are). In many cases, this means that young live streamers can never be totally certain exactly who they are broadcasting to and who is engaging with their live stream.

DISCLOSING PERSONAL INFO

A characteristic of live streaming is the ability for videos to be instantly shared worldwide. Without the correct privacy settings enabled, a child could inadvertently reveal personal information or their location, making them vulnerable to online predators or identity theft. It's wise to regularly check the privacy settings (and what data is being shared) on any apps your child has signed up for.

ANYTHING COULD HAPPEN

As the video streams are live, children might encounter (or inadvertently share) inappropriate content. Most live-streaming apps have rules to prevent this and monitor their services, also providing report buttons where content can be flagged for review. It may not be dealt with instantly, however, meaning that your child could be further exposed to harmful content during a live stream.

UNAUTHORISED RECORDINGS

Each live streaming platform stores completed videos for different periods (which some broadcasts are 24 days, for example, while Facebook and YouTube remove them only at the creator's request). Downloading a video, though, doesn't always stop it from being shared: in some cases, screenshots have been illegally recorded (or screenshots taken) by certain viewers and redistributed on other sites.

ROGUE CONTENT CREATORS

Children can also watch other people's live streams, which could inadvertently contain anything at any time (such as nudity, drug use or profanity). Most apps claim to monitor live streams and will stop any that don't adhere to their guidelines – but with millions of streams per day, it's complicated to regulate them all, so children could be exposed to inappropriate content without parents knowing.

DANGER OF GROOMING

There are increasing reports of children being coerced into performing "suggestive acts" by strangers on some live-streaming apps. Due to the lack of verification required for certain apps, almost anyone can sign up to these services (including anonymously or under a false identity). It's vital, therefore, to ensure the correct safety measures are in place before your child begins live streaming.



Advice for Parents & Carers

PUT PRIVACY FIRST

Through the streaming app's settings, switch your child's account to 'private', so only their friends and followers can see their broadcasts. You could also turn off the live chat, shielding your child from any upsetting comments – although viewers' feedback is often seen as an integral part of the fun. Identify any nearby items (such as school uniforms or visible landmarks) that could give away your child's location.

MANAGE MULTISTREAMING

Some apps and sites let users stream their content through multiple social media platforms at once. A broadcast on SteamYard, for example, can be shared on YouTube, Twitch, X and Facebook if the accounts are linked. The privacy settings can differ on each of these, so we'd suggest only streaming via one platform at a time to maintain greater control over who's watching your child's videos.

GET INVOLVED YOURSELF

Research suggests a significant number of streams show a child on their own, often in a supposed safe space like their bedroom. If your child wants to live stream, ask if you could be present because you're interested in how it works. You could even set up your own account to gain a more detailed knowledge of what your child talks about in their live streams – and who they're broadcasting to.

TALK ABOUT LIVE STREAMING

Try to start with positives before discussing potential risks. You could ask which live streaming apps your child likes and how they use them. Do they just watch streams or create their own? Explain why it's unwise to reveal personal information while streaming (even to friends). If you feel your child's too young for live streams, explain your reasoning to them and perhaps agree to review this decision in the future.

CONSIDER THEIR ONLINE REPUTATION

As the broadcasts are live, it often causes the misconception among young people that whatever happens in their video simply 'vanishes' once the stream ends. However, videos can stay online indefinitely or be recorded by other users. It's important that your child understands what they do and say in a live stream could potentially damage their online reputation and, quite possibly, be seen by prospective future employers, colleges or universities.

Meet Our Expert

David Smith is Head of Digital Learning at Thomas's Danish Lane, London. He's been in the EdTech space since 2002/12 for his efforts in the digital transformation of Dulock Town Primary School and Tower Hamlets, he is also a thought leader in education. Certified Trainer and guest lecturer at University College London on the topic of technology across the curriculum.



NOS National Online Safety®
#WakeUpWednesday

*Screenshot taken from www.youtube.com/watch?v=2023/03/02/01/00/00 (redaction of captures of live-streamed child sexual abuse that will be removed)

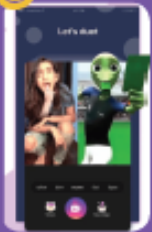


LIKEE (formally known as LIKE) is a free video creation and editing app similar to TikTok. It has a global community of over 200 million users who can create any type of video, add their own special effects and then upload and share them with the world. The app is largely used to create short music videos which users can star in and edit anyway they want using the "Magic Video Maker." Users share their videos on the platform as well as having the option to share across other social media outlets such as Facebook and Instagram. Due to the suggestive content that is available on the app, it has a recommended age of 16+, although the app store rate it as 17+.

AGE RESTRICTION
16+

What parents need to know about

LIKEE



ALL VIDEOS ARE PUBLIC

All user profiles on LIKEE are public which means that every video that is uploaded can be viewed by anyone. This is a privacy setting which can't be changed. In addition, on creating an account, anybody who views your child's video can also download, save and share them, albeit this is a feature which can be turned off. Nonetheless, this places your child's privacy at risk given they can't control who is viewing their videos and potentially sharing them elsewhere.

SEXUAL PREDATORS AND BULLYING

Once a video has been uploaded and shared on LIKEE, anybody can comment on it. There have been reports of sexually suggestive comments made towards children, opening the door to potential child grooming and/or child sexual exploitation risks. Similarly, children may be vulnerable to derogatory or abusive language which could escalate into harassment or bullying.



ACCESS TO INAPPROPRIATE CONTENT

In a Facebook post from April 2019, LIKEE admitted to banning over 400 accounts during a 6 day period due to matters relating to harassment, fraud, pornographic material, violence, gambling and terrorism. There is no safe search feature on the app which means there is a chance your child could potentially watch mature or inappropriate content with relative ease.



EASY FOR MINORS TO SET-UP

Despite the recommended age limit of 16, there are no verification measures in place to help restrict access. Setting up a profile is extremely easy and all that is required is access to a mobile phone. This is a concern for young children who have limited knowledge of how to stay safe online.



PRIVATE MESSAGING

As well as being able to comment publicly, LIKEE also allows users to private message one another. This again opens the door for strangers to contact your child online and build a relationship, this time without being seen. There have been reported cases of sexual grooming and children receiving requests to send inappropriate images via direct message.



DESIGNS TO INCREASE APP USAGE

The more your child engages with the app, the more 'Exp.' they can earn. This in turn can help them achieve higher levels and unlock Privilege to enhance their videos. Similarly, the Leaderboard feature within the app rewards users that receive the most 'likes' every day, again encouraging children to produce more content. Both of these features could contribute towards increased screen time for your child.



ABILITY TO STREAM VIDEOS LIVE

Once a user has achieved a certain level, LIKEE grants them access to stream their videos live with viewers able to engage and post comments as the video is running. This means your child could receive harmful or upsetting comments during a live recording with no filter, as well as viewing other users live streams, which may contain inappropriate or disturbing content.



IN-APP PURCHASES

LIKEE also has a 'Wallet' feature in which users can earn coins during special LIVE events or during their own live streams. They can also purchase diamonds directly from the app for anything between 99p and £99.99, with one tap and one confirmation screen, potentially costing the bill payer a lot of money.



Top Tips for Parents

1 DISABLE OR RESTRICT PRIVATE MESSAGING

The ability to private message one another on LIKEE means that your child could receive messages or media from complete strangers and potentially engage in conversations with people they don't know. In the privacy settings, this feature can be disabled or set to just friends allowing a degree of control over who can privately contact your child.



2 DISABLE ABILITY FOR OTHERS TO SAVE YOUR VIDEOS

Saving and sharing your child's videos to their own device means that anyone could upload and share those videos whenever and wherever they like, without your permission. You can disable this feature in your child's profile settings via the privacy tab.



3 TURN OFF COMMENTS IN PRIVACY SETTINGS

The public nature of LIKEE means that anybody can comment on your child's videos. Whilst many users may be positive and supportive of what your child is doing online, others may be critical or quite nasty. If you are worried about other users and what they may say, you can completely disable comments within the app's privacy settings.



4 BLOCK USERS WHO HARASS, BULLY AND OFFEND

If you are concerned about your child being harassed, bullied or receiving persistent offensive comments from specific users, you can 'block' these individuals. This can be done on the offenders user profile page. Once blocked, the ability to comment on your child's video or private message will be removed although videos will still remain visible.



5 TALK TO YOUR CHILD ABOUT ONLINE DANGERS

Talking to your child about staying safe online will help them stay alert to any potential dangers and give them a more enjoyable experience. Learning how to report inappropriate content and discussing this with your child may ensure they recognise anything malicious and become more vigilant whilst using the app. Similarly, discussing what is acceptable and setting limits on what can and can't be posted online may help to ensure your child avoids any unwanted pitfalls.

6 STICK TO THE RECOMMENDED AGE LIMIT

LIKEE suggest that the recommended age limit for the app is 16+. Reviews of the app suggest that users may post mature or sexually provocative material which isn't tightly regulated and could be accessed or accidentally viewed by your child. Ensuring you adhere to the age limit and encourage your child to be open about what they're viewing will help you keep an eye on what content your child is coming across on the app.



Meet our expert

Pete Bath is a writer with over 10+ years in research and analysis. Working within a specialist area for West Yorkshire Police, Pete has contributed work which has been pivotal in successfully winning high profile cases in court as well as writing as a subject matter expert for industry handbooks.



www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 28.01.2020