

Online Safety Policy



Approved by: Full Governors

Date: July 2026

Last reviewed on: July 2025

Next review due by: July 2027

Change Log:

Date	By Who	Comment
July 2024	S. Baker	Included the use of Smoothwall monitoring facility. Updated online safety lessons/units in line with curriculum changes.
July 2025	S. Baker	Review only
July 2026	S. Baker	Review only

Introduction

This topic may be referred to as Online Safety or e-safety throughout this policy.

What is an Online Safety Policy?

- The school Online Safety policy aims to create an environment where pupils, staff, parents, governors and the wider school community work together to inform each other of ways to use the internet responsibly, safely and positively.
- Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The Online Safety policy encourages appropriate and safe conduct and behaviour when achieving this.
- Pupils, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.
- These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

Ofsted context:

Ofsted have defined e-safety thus (in their previous 'Inspecting e-safety in schools' briefings):

- 'In the context of an inspection, e-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.'

E-safety will be inspected in relation to the following areas:

- 'The behaviour and safety of pupils at the school.'
- 'The quality of leadership in, and management of, the school'

Ofsted have identified three areas of e-safety risk in relation to pupils:

- 'Being exposed to illegal, inappropriate or harmful material.'
- 'Being subjected to harmful online interaction with other users.'
- 'Personal online behaviour that increases the likelihood of, or causes, harm.'

1. Aims and Objectives

- School internet use will be designed for pupil use and include filtering that is appropriate to the age of the pupils.
- School internet uses Smoothwall monitoring to monitor online activity.
- Pupils will be taught what internet use is acceptable and they will be given clear guidelines for its use. (Pupils agree to an Acceptable Use policy when they log on to the school network)
- Pupils will be educated in the effective use of the internet for research; including location, retrieval and evaluation.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information, before accepting its accuracy as well as being taught about disinformation and misinformation.
- Pupils will be taught how to report unpleasant internet content e.g. using the CEOP report abuse icon or Hector protector.

2. Managing Internet Access

2.1 Information System Security

- School ICT system security will be reviewed regularly.
- Virus protection will be reviewed regularly.
- Security strategies will be discussed with the local authority.
- School internet uses Smoothwall monitoring to monitor online activity.

2.2 Email

- Pupils may only use approved school email accounts.
- Pupils must tell a member of staff immediately, if they receive an offensive email.
- In email communication, pupils must not reveal their personal details, or those of others, or arrange to meet anyone.
- Incoming emails should be treated with suspicion and attachments should only be opened if the author is known.
- Emails from pupils to external bodies will be supervised and monitored by an adult.
- The forwarding of chain letters is not permitted.

2.3 Published content and the school website.

- Staff or pupil personal contact information will not be published. The contact details given online will be that of the school office or of staff emails.
- The head teacher will take overall editorial responsibility and ensure content is accurate and appropriate.

2.4 Publishing pupil's images and work.

- Photographs that include pupils will be selected carefully, so that images cannot be misused.
- Pupil's full names will not be used anywhere on the school website, particularly in association with photographs.
- Written permission from parents or guardians will be obtained before photographs of pupils are published on the school website.
- Pupil image file names will not refer to the pupil by name.
- Parents will be clearly informed of the school policy on photographs.

2.5 Social Networking and Personal Publishing

- Social networking sites will not be accessed through the school network.
- Children will be educated on the dangers of social networking sites, their age restrictions and how, when appropriate to use them safely.
- Pupils will be advised never to give out personal details of any kind that may identify them, their friends or location.
- Pupils and parents will be advised that use of the social networking sites brings a range of dangers to primary age pupils.
- Pupils will be advised to use nicknames or avatars, if using social networking sites (when age appropriate).

2.6 Managing Filtering

- The school network operates a filtering system, managed by Trustnet

- The school will work with Trustnet (London Grid for Learning) to ensure systems to protect pupils are reviewed and improved.
 - If staff or pupils come across unsuitable on-line materials, the site must be reported to the online safety co-ordinator/ Network Manager and/or the safeguarding lead.
 - SMT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
 - The school works with NetworkIT24 who provide network support and monitoring.
 - Smoothwall provide monitoring of online activity.
- 2.7 Managing Emerging Technologies
- Emerging technologies will be assessed for their benefits and for any potential risks.
 - Mobile phone use will not be allowed in school when children are present (see mobile phone use policy).
 - If children bring a mobile phone to school for safety when travelling home (Year 6) they will be stored in the front office during the school day.
 - Visitors and new staff are made aware of the mobile phone policy when signing in.
- 2.8 Artificial Intelligence (See AI usage Policy)
- The school recognises that Artificial Intelligence (AI) technologies, including generative AI tools, are increasingly accessible to children and adults.
 - At Cape Primary School we have agreed the use of Copilot in school through Microsoft 365.
 - Pupils will be taught about the safe, responsible and age-appropriate use of AI technologies.
 - Staff will educate pupils about the risks associated with AI-generated content, including misinformation, disinformation, deepfakes, bias, inaccurate information and manipulated media.
 - AI tools used within school will be assessed for safeguarding, privacy and educational suitability before implementation.
 - Staff must not input confidential, personal or sensitive school information into AI systems.
 - Pupils will be taught to critically evaluate information generated by AI and understand that AI-generated content may not always be accurate or reliable.
 - The use of AI to create harmful, inappropriate, abusive or misleading content will be treated as a safeguarding concern and managed in line with school behaviour and safeguarding procedures.
3. Policy decisions
- 3.1 Authorising Internet Access
4. Parents will sign and return safety an internet agreement as part of the home/school agreement.
5. Lessons involving internet access will include a specific online safety element.
6. Children will be directed to appropriate sites, where possible, and internet access will only be under adult supervision.
- 6.1 Assessing Risks
7. The school will take reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of the internet, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school or Sandwell LA can accept liability for any material accessed.
8. The school will monitor online safety and check that the policy is relevant and implementation is appropriate and effective.
- 8.1 Handling online safety complaints
9. Complaints of internet misuse will be dealt with by SMT.
10. Any complaint about staff misuse must be referred to the headteacher.
11. Complaints of a safeguarding nature must be dealt with in accordance with the school's safeguarding procedures.
12. Clear and transparent procedures exist for monitoring, logging, reporting incidents, evaluating, improving and measuring the impact of e-safety. All staff, parents, pupils, contractors and governors know how to report an online safety incident.
13. Introducing Online Safety to pupils
14. Online safety rules will be on display in rooms where computers are used.
15. The home/school agreement will include online safety rules
16. Online safety training will be delivered through computing lessons, PSHE, assemblies, Safer Internet week and online training.

17. Online safety provision is always designed to encourage positive behaviour and practical real world strategies for all members of the school and wider school community.
 18. Online safety will be covered through Project Evolve knowledge maps which will then inform online safety lessons to be taught as well as online safety lessons links to class computing topics.
 19. Online safety will also be taught through PSHE e.g. how to deal with cyber bullying, how to report cyber bullying, and the social effects of spending too much time online.
 20. Online safety events will take place – such as 'Safer Internet' week, 'Anti-Bullying Week' and 'AI Awareness Day'.
 21. Pupils will agree to an Acceptable Use policy when they use the computer and are required to use school internet and computer systems in agreement with the terms specified in the school Acceptable Use policy.
 22. Pupils will be informed that the network and internet use will be monitored and appropriately followed up.
 23. Pupils need to be aware of how to report online safety incidents in school, and how to use external reporting facilities, such as the CEOP report abuse button.
 24. Pupils need to be aware that the school Acceptable Use policy covers all computer, internet and gadget usage in school.
 25. Pupils need to be aware that their internet use out of school on social networking sites is covered under the Acceptable Use policy if it impacts on the school and/or it's staff and pupils in terms of cyber bullying, reputation or illegal activities.
26. Staff and Online Safety
27. All staff understand online safety issues and that online safety is a school priority.
 28. Teachers and teaching support staff will ensure that they are aware of the current school online safety policy, practices and associated procedures for reporting online safety incidents
 29. School senior management is responsible for determining, evaluating and reviewing online safety policies to encompass teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors, and agreed criteria for acceptable use by pupils, school staff and governors.
 30. Training in online safety is provided to all staff.
 31. All staff will read and accept the online safety policy.
 32. Staff will include online safety in planning their Computing lessons.
 33. Staff will be made aware of the importance of monitoring network and internet use.
 34. Staff will use child friendly searches on the internet and teach children about trustworthy internet sites.
 35. NetworkIT 24 are responsible for maintaining the school's networking, IT infrastructure and hardware. They need to be aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet is secure. They need to further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorized external access, with particular regard to external logins and wireless networking.
 36. Support staff also need to maintain and enforce the school's password policy and monitor and maintain the internet filtering.
 37. All staff need to ensure that they are mindful when using social media, in regard to external off site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on internet school messaging or communication platforms, for example email, forums and the school website (see the staff handbook).
 38. All teaching staff need to rigorously monitor pupil internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, tablets and other gadgets on the school site.
 39. Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
 40. Internet usage and suggested websites should be pre-vetted and documented in lesson planning
 41. Staff must be aware of their responsibilities under the General Data Protection Regulation of May 2018 and ensure that personal and sensitive data is securely processed. Any such data sent electronically should be encrypted (See the Data Protection policy). All staff should use encrypted storage systems (memory sticks) if they must store sensitive data. If possible these details are to remain on the school system and not be transferred.

42. Online Safety Roles and Responsibility

6.1 Online Safety Co-ordinator: Georgia Mawdsley

Network Management – SIPS -MiS support and HCSS support, NetworkIT24 network management support.

Designated Safeguarding Person (DSP): Wendy Richmond
Head Teacher: Sally Baker
Governors: The Provisions Committee

6.2 Co-ordinating Online Safety

43. The school has a designated Online Safety Co-ordinator [Under role of Computing Co-ordinator] who works with the Designated Safeguarding Person (DSP) and reports to the SLT and Governors and co-ordinates online safety provision across the school and wider school community.
44. The school uses the online360 safety tool to audit and review provision and identify action points.
<https://360safe.org.uk/>
45. The school Online Safety co-ordinator is responsible for online safety issues on a day to day basis and also liaises with LA contacts, filtering and website providers and school ICT support.
46. The school Online Safety co-ordinator audits and assesses INSET requirements for staff, support staff and governor online safety training, and ensures that all staff are aware of their responsibilities and the school's online safety procedures. The co-ordinator is also the first port of call for staff requiring advice on online safety matters.
47. Although all staff are responsible for upholding the school online safety policy and safer internet practice, the Online Safety co-ordinator, the Designated Safeguarding Person (DSP) and ICT support are responsible for monitoring internet usage by pupils and staff, and on school machines, such as laptops, used off-site.
48. The network manager will always take into account the needs of the users – i.e. the pupils and teachers. It is the responsibility of the network manager to implement online safety effectively without restricting or altering the requirements of the users.
49. The network manager will carry out regular audits and evaluations of the school IT network and should maintain an ongoing development plan for IT provision.
50. Servers, network switches, hubs, Cat5 or Fibre Optic cabling, wireless transmitters, bridges, access points and other physical architecture should be secured to prevent unauthorised or untraceable network access.
51. The DSP will differentiate which online safety incidents are required to be reported to CEOP, local Police, LADO, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.

6.2 Governor's responsibility for online safety

52. The Governors provisions committee will be responsible for online safety to coincide with their safeguarding responsibility.
53. The school Online Safety co-ordinator will liaise directly with the provisions committee with regard to reports on online safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community.
54. Enlisting parents and carers support
55. Parents will sign the home/school agreement which contain the online safety rules.
56. Parents' and carers' will be aware of online safety through workshops, website information, newsletters and online safety activities.
57. It is expected that parents and guardians will support the school's stance on promoting good internet behaviour and responsible use of IT equipment both at school and at home.
58. The school expects parents and guardians to sign the home/school agreement, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as extranets, websites, forums and social media.
59. The school will provide opportunities to educate parents with regard to online safety.

60. Policies to be used alongside the Online Safety Policy
61. Safeguarding Policy
62. Keeping Children Safe in Education
63. Computing policy
64. Anti- Bullying Policy
65. PSHE &C Policy
66. AI Policy

KCSiE 2021 talks about alignment of a selection of policies to the school's Safeguarding Policy and that they should not be applied in isolation; schools must use a 'joined up' approach to Safeguarding procedures and ethos in school. Policies to be aligned with the school's Safeguarding Policy are: Behaviour; Code of Conduct; Online Safety; Anti-bullying; and PSHE. After the 'Everyone's Invited#' investigation and their report in June 2021 'Review of Sexual Abuse of School and Colleges'; additional guidance was sent out to school and colleges:

In our Computing and online safety lessons, we aim to teach children about keeping themselves safe online. The new Sexual Violence and Sexual Harassment document is encapsulated in our curriculum and is captured in our Safeguarding across the curriculum document. As technologies change and expand, children are able to quickly access inappropriate materials through many different digital platforms. In alignment with our PSHE teaching, it is important that we understand our duties in protecting our children but also making them resilient and open to reporting any concerns they have to a trusted adult.

Online behaviours

At Cape Primary School, we understand that harassment and abuse can happen online as well as in person. Whilst we know that at school we follow a curriculum that delivers safeguarding online guidance and support to our pupils, we also acknowledge that our children will spend time at home on their own devices accessing the internet, online chat and social platforms, having access to potential 'inappropriate sexualised images, language and violence'. We will ensure we maintain a vigilance in school in listening out for 'indicators' or receiving concerns from their friends and peers, alongside sharing any images online that our children have accessed any inappropriate materials online or have taken part in any chat groups that are inappropriate for their age or with strangers they do not know. Our staff will ensure that they report any reports or concerns raised to the DSL or Deputy DSL immediately so that action can be taken and parents can be informed straight away and offered advice on how to act. Dependent on the nature of the concern, there might be an offer of Early Help, or a referral to Sandwell Children's Trust or to the Police.

Definitions:

Sexual violence means rape, assault by penetration, or sexual assault (intentional sexual touching). Sexual harassment means unwanted conduct of a sexual nature – such as sexual comments, sexual jokes or taunting, physical behaviour like interfering with clothes, or online harassment such as sexting.

Please note that sexual violence and harassment can take place in homes, schools, out in the community and online.

Unacceptable behaviours:

- All staff should be aware that children can abuse other children (often referred to as peer on peer abuse). And that it can happen both inside and outside of school or college and online. It is important that all staff recognise the indicators and signs of peer on peer abuse and know how to identify it and respond to reports.
- All staff understand, that even if there are no reports in their schools or colleges it does not mean it is not happening, it may be the case that it is just not being reported. As such it is important if staff have any concerns regarding peer on peer abuse they should speak to their designated safeguarding lead (or deputy).
- All staff at Cape Primary School understand the importance of challenging inappropriate behaviours between peers, that are actually abusive in nature. Downplaying certain behaviours by

staff is not acceptable, for example dismissing sexual harassment as “just banter”, “just having a laugh”, “part of growing up” or “boys being boys” can lead to a culture of unacceptable behaviours, an unsafe environment for children and in worst case scenarios a culture that normalises abuse leading to children accepting it as normal and not coming forward to report it. Staff members will report all concerns.

Peer on peer abuse is most likely to include, but may not be limited to:

- bullying (including cyberbullying, prejudice-based and discriminatory bullying);
- abuse in intimate personal relationships between peers;
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm (this may include an online element which facilitates, threatens and/or encourages physical abuse);
- sexual violence, such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence);
- sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse;
- causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party;
- consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery);
- upskirting, which typically involves taking a picture under a person’s clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm; and
- initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).

Process for responding to reported incidents:

At Cape Primary School, all incidents will be reported to the DSL or Deputy DSL via a concerns form. They will in turn investigate the concerns raised and apply one of these measures:

- Manage the incident internally
- Refer to early help
- Refer to children’s social care
- Report to the police

Parents of both the victim or the perpetrator(s) will be informed, unless by doing so will put a child in harms way.

A ‘zero-tolerance’ approach at Cape Primary School:

In receiving raised concerns, regarding any sexual harassment and violence behaviours, we are clear that we will not tolerate these behaviours at our school. We would however, like to emphasise that we will not demonise anyone – we will support and listen to all of the pupils involved. This will include the alleged perpetrator(s) who will be offered support, so that they can change their behaviour. Our response will be:

- Proportionate
- Considered
- Supportive
- Decided on a case-by-case basis

Taking the wishes of the victim(s) into account:

If an incident of sexual harassment or violence has taken place in school, home or the community, school will ensure that victims are kept at a reasonable distance from the alleged perpetrator(s) while on school premises (including during any before or after school-based activities).

In some cases, it might be that victims prefer that the alleged perpetrator(s) move class, whereas others may prefer that they stay in their class but just not sitting next to them. For example, if a victim is afraid of how the friends of the alleged perpetrator(s) might react if their friend was removed from class, the victim might prefer to not be put in this situation.

In discussions with the victim(s), at Cape Primary School we will ensure that we listen to the victim(s) and that their wishes will help us to inform our response, but the DSL/Deputy DSL will make the final decision.

1. A 'culture of respect' at Cape Primary School
2. Our school ethos and behaviour policy help to underpin a culture of respect at our school. The input of our children in helping to construct our behaviour policy and also our anti-bullying scheme 'Stop! I don't like it!' are pivotal in supporting our pupils in reporting any incidents of abuse and harassment. come forward. Our culture and ethos of respect, tolerance, acceptance and diversity will help all pupils to call out incidents and make it harder for anyone to get away with sexist or inappropriate sexual behaviour. In light of a wider societal culture of victim blaming, pupils may be afraid of how reporting incidents of abuse and harassment reflects on them. This can especially be linked to online platforms and social media, as well as in person.

Sanctions to be applied:

At Cape Primary School we will apply different sanctions will be appropriate for different 'levels' of sexual harassment and sexist comments. These sanctions will be:

A verbal warning and an apology to their peer with a verbal explanation to parents when collecting

A letter or phone call to parents

Detention - in school invitation and discussion with parents

A period of internal exclusion (length dependent on incident) – potential Early Help support or contacting children's services

Fixed-term (length dependent on incident) or permanent exclusion - Police involvement

Our response to each incident will be proportionate. We will consider:

The age and developmental stage of the alleged perpetrator(s)

The nature and frequency of the alleged incident(s)

How to balance the sanction alongside education and safeguarding support (if necessary, these will take place at the same time)

Smaller incidents at school

Staff must call out behaviour as it happens so this will help all pupils understand what is and isn't OK. If the incident is very 'low level' – for example, a pupil making a comment that staff have reason to believe they don't fully understand – it may be appropriate to explain why it wasn't OK and ask the pupil to apologise to the victim on the spot. Staff could use this as an opportunity to engage class discussion on being respectful and using inappropriate language.

If the pupil apologises, staff must keep an eye out for any recurrence from that particular pupil.

If they refuse, staff members must escalate the incident to a more serious sanction.

Parents must be informed every time of any low-level incidents, so that this can be addressed at home in conjunction with school, thus helping ensure all parties are on board to help and find a solution going forward, in order change inappropriate to appropriate behaviours.

Support for the alleged perpetrator(s)

At Cape Primary School, we understand that sometimes when pupils demonstrate harmful sexual behaviour (HSB) towards one another, it's because they're communicating their own experience of abuse. We will offer them a safe space to explain what may have happened to them, and to discuss how their actions weren't appropriate. We will gently but firmly condemn the behaviour, not the pupil – otherwise they won't feel safe to open up about their own experiences. We refer them to appropriate agencies such as Creative Therapy or counselling services to help them modify their behaviours. We will use the agencies and toolkits outlined in KCSiE paragraph 464, alongside our Local Authority Support packages.

67. Policy Review Schedule

68. This policy was approved by governors and staff and is stored on the school network and is published for parents and the wider community on the school website.

69. The Online Safety policy will be monitored annually.

70. The Online Safety policy will be reviewed and evaluated in light of online safety incidents or changes in legislation.