



Defence
Children
Services

DCS Directive 3.2.32 Online Safety in DCS Schools and Settings

September 2026 v1.0

General

Authorisation	Head DCS
Senior Responsible Owner	SAFO
Point of Contact	DCS POLRA
Review Date	September 27
Related Policy/Guidance	DCS Policy Directive 7.1.1 Data Protection
	DCS Policy Exclusion Policy
	DCS Policy Directive 3 2 1 Safeguarding
	DfE Teaching Online Safety in Schools 2023
	DCS Policy Directive 3.2.8 Complaints Procedure for DCS Schools and Settings Overseas
	DfE Keeping Children Safe in Education 2025

Commented [S1]: Add in the new exclusion policy here

Commented [JL2]: The behaviour directive has a section on 'reasonable force' (section 11.1)

Aim

1. DCS schools and settings aim to:
 - a. Have robust processes in place to ensure the online safety of pupils, staff, volunteers and SGC members.
 - b. Identify and support groups of pupils that are potentially at greater risk of harm online than others.
 - c. Deliver an effective approach to online safety, which empowers leaders to protect and educate the whole school community in its use of technology, including mobile and smart technology.
 - d. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
2. DCS schools and settings consider the following areas of online safety:
 - a. **Content** – being exposed to illegal, inappropriate or harmful content, such as but not limited to pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny/misandry, self-harm, suicide, prejudice based on faith or belief, radicalisation and extremism.
 - b. **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes.

- c. **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- d. **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Legislation and guidance

3. This Policy Directive¹ is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:
 - a. Teaching online safety
 - b. Meeting digital and technology standards
 - c. Preventing and tackling bullying and cyber-bullying: advice for Head Teachers and school staff
 - d. Relationships and Sex Education (RSE) and health education
 - e. Searching, screening and confiscation
4. It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is 'good reason' to do so.
5. This Policy Directive also considers the National Curriculum computing programmes of study. Academies, including free schools, if applicable, add/amend: This policy complies with our funding agreement and articles of association.

Roles and responsibilities

6. **The Head Teacher/Setting Manager** The Head Teacher/Setting Manager is responsible for making sure that staff understand this document, and that it is being implemented consistently throughout the school or setting. Their responsibility includes:
 - a. Ensuring that all staff undergo online safety training as part of child protection and safeguarding training, and that staff understand the expectations, roles and responsibilities around filtering and monitoring.
 - b. Ensuring that all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are

¹ An EQIA has been completed for this Policy Directive and is available on request.

continually provided with the relevant skills and knowledge to effectively safeguard children.

- c. Co-ordinating regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).
- d. Ensuring that the curriculum includes lessons for pupils to learn how to keep themselves and others safe, including online.
- e. The Head Teacher/Setting Manager has the final decision for escalating concerns and engagement with external agencies where required.

Note: This list is not exhaustive.

7. The Designated Safeguarding Lead (DSL) The DSL takes lead responsibility for online safety in DCS schools and settings, in particular:

- a. Supporting the Head Teacher/Setting Manager in making sure that staff understand this policy and that it is being implemented consistently throughout the school or setting.
- b. Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- c. Providing 1st Lines of Defence Assurance (LoDA) to DCS HQ (SIS) that filtering and monitoring systems are working effectively and reviewed regularly.
- d. Working with the DCS ICT Team to make sure the appropriate systems and processes are in place.
- e. Working with the Head Teacher/Setting Manager, IT Team and other staff, as necessary, to address any online safety issues or incidents.
- f. Managing all online safety issues and incidents in line with the school's child protection policy.
- g. Responding to safeguarding concerns identified by filtering and monitoring.
- h. Making sure that any online safety incidents are logged (**see Annex E**) and dealt with appropriately in line with this policy.
- i. Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- j. Updating and delivering staff training on online safety (**see Annex D**) contains a self-audit for staff on online safety training needs).
- k. Liaising with other agencies and/or external services if necessary.
- l. Providing regular reports on online safety in school to the Head Teacher and/or governing board.

- m. Undertaking annual risk assessments that consider and reflect the risks pupils face
- n. Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.
- o. The DSL holds responsibility for safeguarding decision-making and triage of all online safety incidents logged on CPOMS.

Note: This list is not exhaustive.

8. HQ Defence Children Services The Assistant Head of Rest of World, Assistant Head of Cyprus, AH Educ-Stand PD and Assistant Head of Schools Interface Services must:

- a. Ensure schools and settings have appropriate filtering and monitoring systems in place on school or setting devices and school or setting networks and will regularly review their effectiveness.
- b. Review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, including:
 - i. Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
 - ii. Reviewing filtering and monitoring provisions at least annually,
 - iii. Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
 - iv. Having effective monitoring strategies in place that meet the school's safeguarding needs.

Note: This list is not exhaustive.

9. HQ IT Team (MODSchools) The ICT Team is responsible for:

- a. Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school or settings devices and school or setting networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

- b. Making sure that the school² or setting's³⁴ IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- c. Conducting a full security check and monitoring the school's ICT systems on a regular basis.
- d. Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- e. Making sure that any online safety incidents are logged (**see Annex E**) and dealt with appropriately in line with this policy.
- f. Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

Note: This list is not exhaustive.

10. All staff and volunteers All staff, including contractors and agency staff, and volunteers are responsible for:

- a. Implementing this policy consistently.
- b. Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (**Annex C**) and making sure that pupils follow the school's terms on acceptable use (see **Annexes A and B**).
- c. Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes.
- d. Working with the DSL to make sure that any online safety incidents are logged (**see Annex E**) and dealt with appropriately in line with this policy.
- e. Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the DCS behaviour policy.
- f. Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

Note: This list is not exhaustive.

11. Parents/carers Parents/carers are expected to:

- a. Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy.

² Further guidance for schools from the National Cyber Security Centre is [here](#)

³ Further guidance for Early Years Settings from the National Cyber Security Centre is [here](#)

⁴ National Cyber Security Centre – Practical tips for schools [link](#)

- b. Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see **Annexes A and B**).
- c. Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:
 - i. What are the issues? – [UK Safer Internet Centre](#)
 - ii. Help and advice for parents/carers – [Childnet](#)
 - iii. Parents and carers resource sheet – [Childnet](#)

12. Visitors and members of the community Visitors and members of the community who use the DCS Bring Your Own Device (BYOD) must be made aware of this Policy Directive and are expected to read and comply with it. If appropriate, they will be expected to agree to the terms on Acceptable Use Agreement at **Annex C**.

Educating pupils about online safety

13. Pupils will be taught about online safety as part of the curriculum. Reasonable adjustments for pupils at all stages of education must be made where reasonably practicable and appropriate in accordance with the Equality Act 2010. In Key Stage (KS) 1 pupils will be taught to:
- a. Use technology safely and respectfully, keeping personal information private.
 - b. Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
14. Pupils in Key Stage (KS) 2 will be taught to:
- a. Use technology safely, respectfully and responsibly.
 - b. Recognise acceptable and unacceptable behaviour.
 - c. Identify a range of ways to report concerns about content and contact.
 - d. Be discerning in evaluating digital content.
15. By the end of primary school, pupils will know:
- a. That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure.
 - b. How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this.

- c. That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults.
- d. The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online.
- e. Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up.
- f. That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

16. In KS3, pupils will be taught to:

- a. Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- b. Recognise inappropriate content, contact and conduct, and know how to report concerns

17. Pupils in KS4 will be taught to:

- a. Understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- b. Report a range of concerns.

18. By the end of secondary school, pupils will know:

- a. Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- b. Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues.
- c. The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online.
- d. Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should

understand the serious risks of sending material to others, including the law concerning the sharing of images.

- e. That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery.
- f. The potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment.
- g. How to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared.
- h. That sharing indecent images of people over 18 without consent is a crime.
- i. What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online.
- j. About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them.
- k. That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny/misandry, violence or use of weapons.
- l. Where to go for advice and support about something they have seen online.
- m. That online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong.
- n. That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice.
- o. How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns.
- p. That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic/misandrist behaviours and attitudes which can negatively influence those who see it.
- q. How information and data is generated, collected, shared and used online.

- r. That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising).
 - s. That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion.
 - t. That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk.
19. Pupils will be taught practical cyber security skills including age-appropriate training on safe internet use such as:
- a. Methods that hackers use to trick people into disclosing personal information.
 - b. Password security.
 - c. Social engineering.
 - d. The risks of removable storage devices (e.g. USBs).
 - e. Multi-factor authentication.
 - f. How to report a cyber incident or attack.
 - g. How to report a personal data breach.
 - h. Age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

Educating parents/carers about online safety

20. The school or setting must raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via the DCS website⁵. This Policy Directive must also be shared with parents/carers and be covered during parents' evenings. Reasonable adjustments must be made where reasonable and appropriate in accordance with the Equality Act 2010. The school or setting will let parents/carers know:
- a. What systems the school uses to filter and monitor online use.
 - b. What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

⁵ [Link](#)

- c. If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Teacher and/or the DSL.
- d. That any concerns or queries about this Policy Directive can be raised with any member of staff or the Head Teacher/Setting Manager.

Cyber-bullying

21. **Definition** Cyber-bullying takes place online, including through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the intentional repeated harming of one person or group by another person or group, where the relationship involves an imbalance of power⁶.

22. **Preventing and addressing cyber-bullying** To help prevent cyber-bullying, school or setting leaders must ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. Leaders will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim. Schools and settings must be alert to abuse, harassment and discrimination based on protected characteristics in accordance with the Equality Act 2010.

23. The school or setting must actively discuss cyber-bullying with pupils at a level appropriate for their age. They must explain the possible reasons for it, the forms it may take and potential consequences including for those with protected characteristics. Teaching staff are 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 and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

24. The school or setting must send information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected. Leaflets for school staff can be found

25. In relation to a specific incident of cyber-bullying, the school or setting must follow the processes set out in the DCS Policy Directive 3.2.10 Behaviour in DCS Schools and Settings. the school or setting must use all reasonable endeavours to ensure the incident is contained and handled appropriately.

26. The DSL must report the incident and provide the relevant material to the police⁷ within 24 hours of the incident being discovered if they have reasonable grounds to suspect that possessing that material is illegal. They must also work with external services if it is deemed necessary to do so.

27. **Examining electronic devices** The Head Teacher, and any member of staff authorised to do so by the Head Teacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

Commented [KL3]: @Gill, Craig (RC-DCS-Exec-EdStrat) I would argue that it doesn't need to be repeated with cyber as it can circulate fast on line. I don't think there is necessarily an imbalance of power online it could be a pupil against a teacher for example

Commented [GC4R3]: I would say that the imbalance of power is one person over someone else. Over the internet this can be heightened as it is not face to face. Pupil over pupil can still be one with more power or threat over another. When a child threatens another it can be dismissed but when in writing over a machine it can be taken to heart, read and re read, screenshoted etc.

Commented [KL5]: How do they do this? What should they do

Commented [KL6R5]: @Gill, Craig (RC-DCS-Exec-EdStrat) can you advise please

Commented [KL7]: How and in what timescale?

Commented [GC8R7]: I would say within one working day. If it is serious and needs to go to the police then delay could be dangerous,

⁶ See also the DCS Policy Directive 3.2.10 Behaviour in DCS Schools and Settings

⁷ Further guidance on UK police reporting can be found [here](#), please follow local guidance

- a. Poses a risk to staff or pupils.
 - b. Is identified in the school rules as a banned item for which a search can be carried out.
 - c. Is evidence in relation to an offence.
28. Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
- a. Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Head Teacher / DSL.
 - b. Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it.
 - c. Seek the pupil's co-operation.
 - d. 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.
29. 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:
- a. Cause harm, and/or
 - b. Undermine the safe environment of the school or disrupt teaching, and/or
 - c. Commit an offence
30. If inappropriate material is found on the device, the DSL and / or the Head Teacher must determine the appropriate response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they must first consider the appropriate safeguarding response.
31. To determine if there is good reason to erase data or files from a device, staff members must consider if the material may constitute evidence relating to a suspected offence. In these instances, they must not delete the material, and the device must be handed to the police within 24 hours. If the material cannot be reasonably considered evidence in relation to an offence, staff members may delete it if:
- a. They reasonably consider that its continued existence is likely to cause harm to any person, and/or
 - b. The pupil and/or the parent/carer refuses to delete the material themselves.
 - c. 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:
 - i. Not view the image

- i. Confiscate the device and report the incident to the DSL immediately, who will decide what to do next.
- ii. 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.

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

- a. The DfE's latest guidance on searching, screening and confiscation.
- b. UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- c. DCS behaviour policy / searches and confiscation policy.
- d. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

33. **Artificial intelligence (AI)** Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. DCS recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

34. The Head Teacher or Setting Manager must treat any use of AI to bully pupils very seriously, in line with the DCS Policy Directive 3.2.10 Behaviour in DCS Schools and Settings and the school or setting's Anti Bullying policy. Staff should be aware of the risks of using AI tools while they are still being developed and should always follow the relevant DPIA and Schools AI Protocols.

Acceptable use of the internet in school

35. All pupils, parents/carers, staff, volunteers and SGC are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (**Annexes A, B and C**).

36. Visitors will be expected to read and agree to the school's terms on acceptable use. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. DCS will monitor the websites visited by pupils, staff, volunteers, SGC members and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate. More information is set out in the acceptable use agreements in **Annexes A, B and C**.

Pupils using mobile devices in school

37. As per the DCS Mobile Technology Statement the following will apply:

- a. **Primary School Pupils** Personal Mobile Phones and Technology with image taking capacity are not permitted for use at any time within the primary school. If parents permit children to use these items on the journey to and from the school, the Head Teacher and school staff bears no responsibility for the safety of the device whilst on school grounds.
- b. **Secondary School Students** Personal Mobile Phones (and any form of communication device) are allowed in school but are switched off and out of sight throughout the school day unless the teacher allows their use for an educational purpose. Should any student wish to use their mobile phone during the school day (but not during lesson time) then they are only allowed to do so at the school reception after informing the office staff of who they are calling and why.

Staff using work devices outside school or setting

38. All staff members will take appropriate steps to ensure MOD devices remain secure. This includes, but is not limited to:
- a. Keeping the device password protected as per MOD Policy.
 - b. Making sure the device is locked if left inactive for a period of time.
 - c. Not sharing the device with any other member of staff or family members.
 - d. Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in **Annex C**.
 - e. Work devices must be used solely for work activities.
 - f. If staff have any concerns over the security of their device, they must seek advice from DCS IT Team.
39. The DSL and ICT team will review filtering and monitoring data regularly to ensure systems remain effective in identifying safeguarding risks, including emerging online behaviours and trends. Where gaps or patterns are identified, appropriate action will be taken to strengthen safeguarding responses. Safeguarding records and incident trends will be reviewed periodically to ensure consistency of response, identify emerging risks and inform staff training and curriculum development.

Misuse of ICT or Internet

40. Where a pupil misuses the school's ICT systems or internet, leaders will follow the procedures set out in DCS Direction and Policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
41. Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with staff disciplinary procedures and / or staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

42. In consultation with the relevant Assistant Head of Service, The Chief of Staff and the Head DCS, the Head Teacher will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training for staff, governors and volunteers

43. All new staff members must receive training⁸, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation and appropriate action to be taken. Reasonable adjustments must be made where practicable and appropriate.
44. Training must include recognising and responding to online incidents including in relation to protected characteristics.
45. All staff members must receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). By way of this training, all staff must be made aware that:
- a. Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
 - b. Children can abuse their peers online through:
 - i. Abusive, threatening, harassing and misogynistic/misandrist messages
 - ii. Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - iii. Sharing of abusive images and pornography, to those who don't want to receive such content
 - iv. Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
46. Training will also help staff:
- a. Develop better awareness to assist in spotting the signs and symptoms of online abuse
 - b. Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
 - c. Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.
47. The DSL must undertake child protection and safeguarding training, which must include online safety, at least every two years. They will also update their knowledge and skills relating to online safety at regular intervals, and at least annually. SGC members will receive training on safe internet use and online safeguarding issues as

Commented [KL9]: @Gill, Craig (RC-DCS-Exec-EdStrat) | @Yeoman, Andrew (RC-DCS-SS-AHEducStandPD) | I added this part in I presume we would advise on this?

Commented [GC10R9]: Sorry - being think - we as in DCS or PoLRA? would advise?

Commented [KL11]: @Gill, Craig (RC-DCS-Exec-EdStrat) | I added this are you aware if this is included in training?

Commented [GC12R11]: Yes

⁸ Link to National Cyber Security Centre 'Cyber Security Training for Schools Staff' is [here](#) please also follow school/setting procedure

part of their safeguarding training. Volunteers must receive appropriate training and updates. More information about safeguarding training is set out in the DCS Policy Directive 3.2.1 Safeguarding.

Monitoring arrangements

48. The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found at **Annex E**.

ACCEPTABLE USE SCHOOLS ICT AND INTERNET AGREEMENT
EYFS and KS1 (pupils and parents/carers)
Official-Sensitive Personal when complete

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- a. Ask a teacher or adult if I can do so before using them
- b. Only use websites that a teacher or adult has told me or allowed me to use
- c. Tell my teacher immediately if:
- d. I select a website by mistake
- e. I receive messages from people I don't know
- f. I find anything that may upset or harm me or my friends
- g. Use school computers for schoolwork only
- h. Be kind to others and not upset or be rude to them
- i. Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- j. Only use the username and password I have been given
- k. Try my hardest to remember my username and password
- l. Never share my password with anyone, including my friends
- m. Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- n. Save my work on the school network
- o. Check with my teacher before I print anything
- p. Log off or shut down a computer or other device when I have finished using it
- q. I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

Signed (parent/carer):

Date:

**Annex B to
DCS Directive 3.2.32
Dated September 26**

ACCEPTABLE USE OF SCHOOL ICT AND INTERNET AGREEMENT
KS2, KS3 and KS4 (pupils and parents/carers)
Official-Sensitive Personal when complete

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- a. Always use the school's ICT systems and the internet responsibly and for educational purposes only
- b. Only use them when a teacher is present, or with a teacher's permission
- c. Keep my usernames and passwords safe and not share these with others
- d. Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- e. Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- f. Always log off or shut down a computer when I've finished working on it

I will not:

- a. Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- b. Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- c. Use any inappropriate language when communicating online, including in emails
- d. Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- e. Log in to the school's network using someone else's details
- f. Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- g. If I bring a personal mobile phone or other personal electronic device into school:
- h. I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission

- i. I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
- j. I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):.....

Date:

Parent/carer's agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

**Annex C to
DCS Directive 3.2.32
Dated September 26**

**ACCEPTABLE USE AGREEMENT OF SCHOOL ICT SYSTEMS AND INTERNET
(SGC, Staff, Volunteers and Visitors)
Official-Sensitive Personal when complete**

Name of SGC, staff, volunteer or visitor (delete as applicable)

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- a. Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- b. Use them in any way that could harm the school's reputation
- c. Access social networking sites or chat rooms
- d. Use any improper language when communicating online, including in emails or other messaging services
- e. Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- f. Share my password with others or log in to the school's network using someone else's details
- g. Take photographs of pupils without checking with teachers first
- h. Share confidential information about the school, its pupils or staff, or other members of the community
- i. Access, modify or share data I'm not authorised to access, modify or share
- j. Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me, they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that the pupils in my care do so too.

Signed

Date

(staff member/governor/volunteer/visitor):

**Annex D to
DCS Directive 3.2.32
Dated September 26**

ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF AND VOLUNTEERS
Official-Sensitive Personal when complete

Name:

Date:

Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

**Annex E to
DCS Directive 3.2.32
Dated September 26**

ONLINE SAFETY INCIDENT REPORT LOG
Official-Sensitive/Personal when complete

Date:	Where the incident took place:	Description of the incident, including whether it was in relation to a protected characteristic:	Action taken:	Name and signature of staff member recording the incident: