Online safety policy 2026

Policy produced by school and LA
Adopted by Governors FGB-Academic year 26/27
Review date- Academic year 27/28

Contents

Key contacts		2
1	Online safety: the issues	
1.1	Introduction	3
1.2	Benefits and risks of technology	3
2	School online safety strategies	
2.1	Whole-school approach	5
2,2	Purpose and description	6
2.3	Roles and responsibilities	7
2.4	Pupils with special needs	10
2.5	Working with parents	11
3	Online safety policies	
3.1	Accessing and monitoring the system	12
3.2	Confidentiality and data protection	12
3.3	Acceptable use policies	13
3.4	Teaching online safety	13
3.5	Staff training and conduct	17
3.6	Safe use of technology	19
4	Responding to incidents	
4.1	Policy statement	25
4.2	Unintentional access by pupils	25
4.3	Intentional access by pupils	26
4.4	Inappropriate IT use by staff	26
4.5	Online bullying	27
4.6	Harmful sexual behaviour online	30
4.7	Inappropriate contacts with adults	31
4.8	Contact with violent extremism	32
4.9	Sites advocating suicide, self-harm and anorexia	33
5	Sanctions for misuse of ICT	
5.1	Pupils	34
5.2	Staff	36
Appendices:		
Appendix 1: Acceptable use policies for primary schools		38
Appendix 2: Acceptable use policies for secondary schools		39
Appendix 3: Acceptable use policies for staff		41

*** italicised font within the model policy indicates text that can be used within a school's own online safety policy.**
Red font indicates changes and additions to this version of the policy

Key contacts

School/college

Name of school/college: St Luke's CE Primary School

Headteacher/principal:
Name: Paul Smith
Contact details: office@stlukesprimary.org.uk

Online safety co-ordinator:
Name: Paul Smith
Contact details: office@stlukesprimary.org.uk

Nominated LGfL contact:
Name: Paul Smith
Contact details: office@stlukesprimary.org.uk

IT systems/Data manager:
Name: Adam Thornton
Contact details: office@stlukesprimary.org.uk

Designated safeguarding lead:
Name: Paul Smith
Contact details: office@stlukesprimary.org.uk

Nominated governor:
Name: Judy Powell
Contact details: office@stlukesprimary.org.uk

London Borough of Westminster

Local Authority Designated Officer (LADO)
Name: Aqualma Daniel
Contact: 07870 481712
Email: LADO@westminster.gov.uk

Child and Family Contact/MASH team:
Service Manager: Catherine Hoy
Tel: 020 7641 5428

Prevent Co-ordinator/ Education Manager
Name: Abdul Yusuf
Tel: 0781 705 4699

1 Information on internet technology

1.1 Introduction

The educational and social benefits for children in using the internet should be promoted, but this should be balanced against the need to safeguard children against the inherent risks from internet technology. Further, schools need to be able to teach children how to keep themselves safe whilst on-line.

This document provides schools with guidance on developing an effective online safety strategy so that these aims to be achieved and support staff to recognise the risks and take action to help children use the internet safely and responsibly.

Schools should have a strategy in place for communicating the online safety policy to staff, pupils and parents and the policy document should be posted on the school's website.

1.2 Benefits and risks

Computing covers a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, children need to learn computing skills in order to prepare themselves for the working environment and it is important that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of computing need to be harnessed to enhance children's learning.

The risk associated with use of technology by children can be grouped into 4 categories.

1.2.1 Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour, and misinformation, disinformation (including fake news) and conspiracy theories, that they are unable to evaluate in a critical manner.

1.2.2 Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and

can hide their identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a child or for child on child abuse. More details on this can be found in section 4.5 of this policy.

1.2.3 Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

1.2.4 Conduct

Conduct refers to online behaviour that increases the likelihood of harm, including cyberbullying, making or sharing nude or semi-nude images (including AI-generated images), online harassment, sexualised behaviour, abusive communications and other online behaviours that place children or others at risk.

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- using information from the internet in a way that breaches copyright laws
- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- online bullying and child on child abuse (see section 4.5 for further details)

- use of mobile devices for the purposes of sexual harassment such as making or sharing nude and semi-nude images, including AI-generated images where applicable that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

2 School online safety strategies

2.1 Whole school approach

Computing is now a key part of the school curriculum as well as a key element of modern communications technology that is widely used, and one of the key aims of computing is to ensure that pupils are aware of online safety messages. This is part of the school's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment.

Schools should consider the following in order to ensure a holistic approach to online safety:

- Staff should be aware that online safety is an element of many safeguarding issues as technology can be used to aid many forms of abuse and exploitation, for example sexual harassment and cyberbullying, and should be aware of the use of technology in child on child abuse.

- When developing new policies, schools should ensure online safety and the impact of technology is considered and what safeguards need to be put in place, for example when developing policies around behaviour and staff conduct.

- Schools should ensure that consistent messages are given to staff and pupils and that everyone understands the online safety policy: staff

should receive suitable training around online safety and similar messages should be taught to pupils.

- Staff should be aware of the importance of ensuring their own use of technology complies with school policies, particularly in terms of contact with pupils, and schools must ensure there are clear policies available to staff on expectations for online behaviour.

- There should be a clear link between the online safety policy and the behaviour policy that sets out expected standards for pupil's online behaviour and expected sanctions for breaches.

- School's online safety policies should be reviewed regularly and staff training refreshed in order to ensure that they remain relevant in the face of changing technologies.

- Schools should undertake an annual online safety risk assessment to identify emerging risks, evaluate existing controls and inform future development of online safety policy, training and curriculum provision.

- Schools should be aware of the potential safety risks of using Generative AI and should take note of guidance on their responsibilities and on mitigating risks.

Generative artificial intelligence (AI) in education - GOV.UK
Using AI in education settings: support materials - GOV.UK

Schools should refer to:

DfE non-statutory guidance on teaching online safety:
https://www.gov.uk/government/publications/teaching-online-safety-in-schools

DfE statutory guidance on RSE:
https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

DfE guidance for schools on planning technology
Plan technology for your school - GOV.UK

2.2 Purpose and description

Schools should have an online safety strategy in place based on a framework of policy, practice, education and technological support that ensures a safe

online learning environment that maximises the educational benefits of ICT whilst minimising the associated risks. Its purpose is to:

- promote the use of technology within the curriculum
- protect children from harm
- safeguard staff in their contact with pupils and their own use of the internet
- ensure the school fulfils its duty of care to pupils
- provide clear expectations for staff and pupils on acceptable use of the internet.

In particular schools must ensure the following:

- A ***safe internet platform*** that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems (for example the London Grid for Learning platform).
  This includes robust filtering and monitoring systems that comply with the Department of *Education Filtering and monitoring standards for schools and colleges.*

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

Schools/colleges may also use resources available on the London Grid for Learning website to help them to monitor their systems.
Home Page - London Grid for Learning (lgfl.net)

Schools should take steps to ensure that IT systems are robust enough to prevent data breaches and can protect pupil's personal information. The following cyber security guidance can help schools to prevent breaches and mitigate risks.
Meeting digital and technology standards in schools and colleges - Cyber security: core standard - Guidance - GOV.UK
Cybersecurity – What If? « NEN
Cyber security training for school staff | National Cyber Security Centre

- A culture of ***safe practice*** underpinned by a strong framework of online safety policy that ensures everyone is aware of expected standards of on-line behaviour.

- Children are ***taught to keep themselves and others safe*** on-line and use technology responsibly; this should be achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

2.3 Roles and responsibilities

A successful online safety strategy needs to be inclusive of the whole school community, including teaching assistants, supervisory assistants, governors and others, and forge links with parents and carers. The strategy must have the backing of school governors, should be overseen by the head teacher and be fully implemented by all staff, including technical and non-teaching staff.

2.3.1 Head teacher's role

Head teachers have ultimate responsibility for online safety issues within the school including:

- *the overall development and implementation of the school's online safety policy and ensuring the security and management of online data*
- *ensuring that online safety issues are given a high profile within the school community*
- *linking with the board of governors and parents and carers to promote online safety and forward the school's online safety strategy*
- *ensuring online safety is embedded in staff induction and training programmes*
- *deciding on sanctions against staff and pupils who are in breach of acceptable use policies and responding to serious incidents involving online safety.*

2.3.2 Governors' role

Governing bodies have a statutory responsibility for pupil safety and should therefore be aware of online safety issues, providing support to the head teacher in the development of the school's online safety strategy.

Governors should ensure that there are policies and procedures in place to keep pupils safe online and that these are reviewed regularly.

Governors should liaise with IT staff and service providers to annually review school IT filtering and monitoring systems to check their effectiveness and that filtering is working on all internet-connected devices across the school premises, with a record kept of checks carried out. The annual review should be undertaken jointly by the nominated senior leader, designated

safeguarding lead and IT support provider. Governors should ensure that the school leadership team are aware of what provision is in place and how to escalate any concerns.

Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, governors should always use business email addresses when conducting school business.

2.3.3 Online safety co-ordinator's role

All schools should have a designated online safety co-ordinator who is responsible for co-ordinating online safety policies on behalf of the school. Ideally, the officer should be a senior member of the management team. Given the issues associated with online safety, it is appropriate for the designated safeguarding lead to be the school's online safety co-ordinator.

The online safety co-ordinator and designated safeguarding lead should maintain an operational understanding of filtering and monitoring systems; review concerns generated through monitoring systems and ensure any safeguarding concerns identified are acted upon promptly.

The online safety co-ordinator should have the authority, knowledge and experience to carry out the following:

- *develop, implement, monitor and review the school's online safety policy*
- *ensure that staff and pupils are aware that any online safety incident should be reported to them*
- *ensure online safety is embedded in the curriculum*
- *provide the first point of contact and advice for school staff, governors, pupils and parents*
- *liaise with the school's network manager, the head teacher and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems and that the school has appropriate filtering and monitoring systems*
- *assess the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers*
- *raise the profile of online safety awareness with the school by ensuring access to training and relevant online safety literature*

- *ensure that all staff and pupils have read and signed the acceptable use policy (AUP)*
- *report annually to the board of governors on the implementation of the school's online safety strategy*
- *maintain a log of internet related incidents and co-ordinate any investigation into breaches*
- *discuss any breaches of a safeguarding nature with the designated safeguarding lead who will decide whether to refer the matter to the MASH.*

In addition, it is an Ofsted recommendation that the online safety co-ordinator receives recognised training CEOP or E-PICT in order to carry out their role more effectively. In Camden, this is available from the CLC.

2.3.4 Network manager's role

Where schools have one, their role is:

- *the maintenance and monitoring of the school internet system including anti-virus and filtering and monitoring systems*
- *carrying out monitoring and audits of networks and reporting breaches to the online safety co-ordinator*
- *supporting any subsequent investigation into breaches and preserving any evidence.*

Where schools do not have a network manager, support and advice can be provided and the head teacher or a delegated staff member needs to take responsibility for organising this.

2.3.5 Role of school staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for pupils. Their role is:

- *adhering to the school's online safety and acceptable use policy and procedures*
- *communicating the school's online safety and acceptable use policy to pupils*
- *keeping pupils safe and ensuring they receive appropriate supervision and support whilst using the internet*
- *planning use of the internet for lessons and researching on-line materials and resources*
- *reporting breaches of internet use to the online safety co-ordinator*

- *recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the online safety co-ordinator*
- *teaching the online safety and digital literacy elements of the new curriculum.*

2.3.6 Designated safeguarding leads

Where any online safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated safeguarding lead for the school who will decide whether or not a referral should be made to Children's Safeguarding and Family Help or the Police. In some schools, the designated safeguarding lead will be the online safety co-ordinator.

2.4 Pupils with special educational needs and disabilities (SEND)

Pupils with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision. Schools should have a flexible and personalised approach to online safeguarding for these pupils in order to meet their needs.

SEND co-ordinators are responsible for providing extra support for these pupils and should:

- *link with the online safety co-ordinator to discuss and agree whether the mainstream safeguarding systems on the internet are adequate for pupils with SEND*
- *where necessary, liaise with the online safety co-ordinator and the IT service to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of pupils with SEND*
- *ensure that the school's online safety policy is adapted to suit the needs of pupils with SEND*
- *be aware that some pupils with SEND may not have the cognitive understanding to differentiate between fact and fiction online and may repeat content and behaviours in the real world without understanding the consequences*
- *liaise with parents, carers and other relevant agencies in developing online safety practices for pupils with SEND*
- *keep up to date with any developments regarding emerging technologies and online safety and how these may impact on pupils with SEND.*

2.5 Working with parents and carers

It is essential that schools involve parents and carers in the development and implementation of online safety strategies and policies; most children will have internet access at home or own mobile devices and might not be as closely supervised in its use as they would be at school.

Therefore, parents and carers need to know about the risks so that they are able to continue online safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

The school should consider offering online safety training opportunities to parents in order to provide them with information to help them keep their child safe online. Information for parents on online safety can be found on the Camden Safeguarding Children Partnership website: Online Safety - Camden Safeguarding Children Partnership CSCP

The head teacher, board of governors and the online safety coordinator should consider what strategies to adopt to ensure parents are aware of online safety issues and support them in reinforcing online safety messages at home.
Parents should be provided with information on computing and the school's online safety policy when they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour. Parents should also be informed that they can contact the school's online safety co-ordinator if they have any concerns about their child's use of technology.

Where remote online learning is being used, parents should be made aware of what arrangements have been made, which websites children will be accessing and any member of staff they will be interacting with online.

3 Online safety policies

3.1 Accessing and monitoring the system

- *Access to the school internet system should be via individual log-ins and passwords for staff and pupils wherever possible. Visitors should have permission from the head teacher or online safety co-ordinator to access the system and be given a separate visitors log-in.*

- *The online safety co-ordinator should keep a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.*

- *Staff should be required to change their password every 6 months.*

- *Network and technical staff responsible for monitoring systems should be supervised by a senior member of their management team.*

- *The online safety co-ordinator and teaching staff should carefully consider the location of internet enabled devices in classrooms and teaching areas in order to allow an appropriate level of supervision of pupils depending on their age and experience.*

3.2 Confidentiality and data protection

- *The school will ensure that all data held on its IT systems is held in accordance with the principles of the Data Protection Act 2018. Data will be held securely and password protected with access given only to staff members on a "need to know" basis.*
- *Pupil data that is being sent to other organisations will be encrypted and sent via a safe and secure system such as School2School. Any breaches of data security should be reported to the head teacher immediately.*

- *Where the school uses CCTV, a notice will be displayed in a prominent place to ensure staff and students are aware of this and recordings will not be revealed without appropriate permission.*

3.3 Acceptable use policies

- *All internet users within the school will be expected to sign an acceptable use agreement on an annual basis that sets out their rights and responsibilities and incorporates the school online safety rules regarding their internet use.*

- *For primary school pupils, acceptable use agreements will be signed by parents on their child's behalf at the same time that they give consent for their child to have access to the internet in school (see appendix 1).*

- *Secondary school pupils and their parents should both sign the acceptable use policy, and use of the internet in schools is dependent on signing this agreement (see appendix 2).*

- *Staff are expected to sign an acceptable use policy on appointment, and this will be integrated into their general terms of employment (see appendix 3).*

The school's online safety co-ordinator will keep a copy of all signed acceptable use agreements.

3.4 Teaching online safety

3.4.1 Responsibility

One of the key features of the school's online safety strategy is teaching pupils to protect themselves and behave responsibly while on-line. There is an expectation that over time, pupils will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- *Overall responsibility for the design and co-ordination of online safety education lies with the head teacher and the online safety co-ordinator, but all staff should play a role in delivering online safety messages.*

- *The online safety co-ordinator is responsible for ensuring that all staff have the knowledge and resources to enable them to carry out this role.*

- *Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum.*
- *Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons.*

- *The start of every lesson where computers are being used should be an opportunity to remind pupils of expectations on internet use and the need to follow basic principles to keep safe.*

- *Schools are required to teach about online bullying as part of statutory Relationships Education (primary), Relationships and Sex Education (secondary) and health education (all schools).*

- *PSHE lessons provide an ideal for discussion on online safety issues to ensure that pupils understand the risks and why it is important to regulate their behaviour whilst on-line.*

- *Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills for example pupils with SEND.*

- *Teachers should ensure that the school's policy on pupils' use of their own mobile phones and other mobile devices in school is adhered to.*

- *Schools should maintain reporting systems that are well promoted, easy to access and understood by pupils so that concerns can be raised confidently and acted upon promptly.*

3.4.2 Content

Pupils should be taught all elements of online safety included in the computing curriculum so that they:

- *use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies;*

- *can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems;*
- *are responsible, competent, confident and creative users of information and communication technology.*

Primary pupils should be taught all elements of online safety included in Statutory Relationships Education:

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help
- that people sometimes behave differently online, including by pretending to be someone they are not.
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.

- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- how information and data is shared and used online.

Statutory Health Education should include:

- that bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing
- that for most people the internet is an integral part of life and has many benefits.
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- why social media, some computer games and online gaming, for example, are age restricted.
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- how to be a discerning consumer of information online including understanding that information, including that from search engines is ranked, selected and targeted
- where and how to report concerns and get support with issues online.

Secondary pupils should be taught all elements of online safety included in statutory Relationships and Sex Education:

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders to report bullying and how and where to get help.
- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- what to do and where to get support to report material or manage issues online.

- the impact of viewing harmful content
- that specifically sexually explicit material eg pornography presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- how information and data is generated, collected, shared and used online
- online misogyny and misandry, harmful influencers, pornography, deepfake content and other emerging online harms, enabling pupils to critically evaluate and challenge harmful online content.

Statutory Health Education should include:

- the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image, how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online

- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

3.5 Staff training and conduct

3.5.1 Training

- *All school staff and governors should receive training with regard to IT systems and online safety as part of their induction and this should include a meeting with the online safety co-ordinator and the network manager.*

- *Staff should also attend specific training on online safety available from the CSCP so that they are aware of the risks and actions to take to keep pupils safe online. School management should ensure that staff*

attend regular update training in order to ensure they can keep up with new developments in technology and any emerging safety issues.

Training must include online safety, cyber security awareness, the school's filtering and monitoring arrangements, generative AI risks and the safeguarding implications of emerging technologies. Staff will receive safeguarding and online safety updates at least annually and more frequently where required.

Camden City Learning Centre offers whole school training including updates as well as training for governors and parents.

3.5.2 IT and safe teaching practice

School staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils. Staff should refer to the model social media policy for school staff available on the CSCP schools safeguarding policies page for further guidance.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- *Photographic and video images of pupils should only be taken by staff in connection with educational purposes, for example school trips.*
- *Staff should always use school equipment and only store images on the school computer system, with all other copies of the images on personal mobile devices erased.*
- *Staff should take care regarding the content of and access to their own social networking sites and ensure that pupils and parents cannot gain access to these.*
- *Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.*
- *Staff should be particularly careful regarding any comments to do with the school that are communicated over the internet; remarks that are*

private may go to a wider audience and raise questions regarding confidentiality.

- *Staff should not post any comments about specific pupils or staff members on their social networking sites or any comments that would bring the school or their profession into disrepute.*

- *Staff should not engage in any conversation with pupils via instant messaging or social networking sites as these may be misinterpreted or taken out of context.*

- *Where staff need to communicate with pupils regarding school work, this should be via the school email system and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.*

- *When making contact with parents or pupils by telephone, staff should only use school equipment. Pupil or parent numbers should not be stored on a staff member's personal mobile phone and staff should avoid lending their mobile phones to pupils.*

- *When making contact with parents or pupils by email, staff should always use their school email address or account. Personal email addresses and accounts should never be used.*

- *Staff should ensure that personal data relating to pupils is stored securely and encrypted if taken off the school premises.*

- *Where staff are using mobile equipment such as laptops or tablets provided by the school, they should ensure that the equipment is kept safe and secure at all times.*

3.5.3 Exit strategy

When staff leave, their line manager should liaise with the network manager to ensure that any school equipment is handed over and that PIN numbers, passwords and other access codes to be reset so that the staff member can be removed from the school's IT system.

3.6 Safe use of technology

The school recognises that generative AI presents safeguarding risks including deepfakes, AI-generated nude and semi-nude imagery,

misinformation, manipulation and impersonation. Staff and pupils will be taught how to identify and respond to these risks and the school's filtering and monitoring systems will be reviewed to ensure appropriate protection from AI-related harms.

3.6.1 Internet and search engines

- *When using the internet, children should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk.*
- *Primary school children should be supervised at all times when using the internet. Although supervision of secondary school pupils will be more flexible, teachers should remain vigilant at all times during lessons.*

- *Pupils should not be allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose.*

- *Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.*

- *Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the online safety co-ordinator, who will liaise with the IT service provider for temporary access. Teachers should notify the online safety co-ordinator once access is no longer needed to ensure the site is blocked.*

3.6.2 Evaluating and using internet content

Teachers should teach pupils good research skills that help them to maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

3.6.3 Safe use of applications

***School email systems** should be hosted by an email system that allows content to be filtered and allow pupils to send emails to others within the school or to approved email addresses externally.*

***Social networking sites** such as Facebook, Instagram and Twitter allow users to publish information about them to be seen by anyone who has*

access to the site. Generally, these would have limited use in schools but pupils are likely to use these sites at home.

Online communities and forums *are sites that enable users to discuss issues and share ideas on-line. Some schools may feel that these have an educational value.*

Chat rooms *are internet sites where users can join in "conversations" on-line;* ***instant messaging*** *allows instant communications between two people on-line. In most cases, pupils will use these at home although school internet systems do host these applications.*

Gaming-based sites *allow children to "chat" to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to children. Consequently such sites should not be accessible via school internet systems.*

Safety rules

- *Access to and use of personal email accounts, unregulated public social networking sites, chat rooms or gaming sites on the school internet system is forbidden and is usually blocked. This is to protect pupils from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.*

- *If schools identify a clear educational use for emails or social networking sites and forums for on-line publishing, they should only use approved sites such as those provided by the IT service provider. Any use of these sites should be strictly supervised by the responsible teacher.*

- *Emails should only be sent via the school internet system to addresses within the school system or approved external address. All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.*
- *Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the online safety co-ordinator who will liaise with the learning platform provider.*

- *Apart from the head teacher, individual email addresses for staff or pupils should not be published on the school website.*

- *Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.*

- *Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.*

- *All electronic communications should be polite; if a pupil receives an offensive or distressing email or comment, they should be instructed not to reply and to notify the responsible teacher immediately.*

- *Pupils should be warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment.*

- *Users should be aware that as use of the school internet system is for the purposes of education or school business only, and its use may be monitored.*

- *To teach pupils to stay safe online outside of school, they should be advised:*

    - *not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended*
    - *to only use moderated chat rooms that require registration and are specifically for their age group;*
    - *not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them*
    - *how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them*
    - *to behave responsibly whilst on-line and keep communications polite*
    - *not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.*
    - *not to give out personal details to anyone on-line that may help to identify or locate them or anyone else*

- *not to arrange to meet anyone whom they have only met on-line or go "off-line" with anyone they meet in a chat room*
- *to behave responsibly whilst on-line and keep communications polite*
- *not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.*

3.6.4 Video calling and remote learning

Video calling or live streaming enables users to communicate face-to-face via the internet using web cameras.

Schools should have a remote learning policy and should refer to the DfE and London Grid for Learning guidance for advice on what to include. The following should be taken into account:
https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

- *only using school registered accounts rather than personal accounts*
- *recording remote learning for safeguarding purposes*
- *the security of the video link*
- *checking settings regularly to ensure teachers have full control of the meeting ie; who can start, join or chat in the stream*
- *paying attention to background settings to prevent breach of privacy*
- *training for teachers to use the new technology*
- *a system for teachers to log any remote learning contacts and issues.*

Further guidance on remote learning can be found on the London Grid For Learning website: https://www.lgfl.net/online-safety/

3.6.5 School website

- *Content should not be uploaded onto the school website unless it has been authorised by the online safety co-ordinator and the head teacher, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.*

- *Schools should designate a named person or persons to have responsibility for uploading materials onto the website. This is particularly important where a school allows a number of staff members to upload information onto the website.*

- *To ensure the privacy and security of staff and pupils, the contact details on the website should be the school address, email and telephone number. No contact details for staff or pupils should be contained on the website.*

- *Children's full names should never be published on the website.*

- *Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.*

3.6.6 Photographic and video images

- *Where the school uses photographs and videos of pupils for publicity purposes, for example on the school website, images should be carefully selected so that individual pupils cannot be easily identified. It is recommended that group photographs are used.*

- *Where photographs or videos of children are used, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear.*

- *Children's names should never be published where their photograph or video is being used.*

- *Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.*

- *Images should be securely stored only on the school's computer system and all other copies deleted.*

- *Stored images should not be labelled with the child's name and all images held of children should be deleted once the child has left the school.*

- *Staff should not use personal devices to take photographs of pupils.*

- *Schools should inform parents that although they may take photographic images of school events that include other children, it is on the understanding that these images are for personal use only and will not be published on the internet or social networking sites.*

3.6.7 Pupils own mobile devices

It is now an expectation that pupils do not have access to mobile devices during the whole school day unless an exception has been agreed. Schools should have a strategy in place to ensure a mobile-free environment and set out the circumstances for any exceptions. For further information please refer the government guidance.
Creating a mobile phone-free environment: school case studies - GOV.UK

Schools should also consider what policy to apply to staff use of their own devices whilst at school.

In the event that a pupil's device is used for bullying or sexual harassment, schools should have a policy in place allowing the device to be confiscated so that evidence can be gathered. Schools should refer to the government guidance available at: https://www.gov.uk/government/publications/searching-screening-and-confiscation

Individual schools take note of the *Camden model Screening and searching guidance for schools* available on the CSCP schools safeguarding policies webpage.

Schools should record their policy here and may wish to refer to the Department of Education guidance for further information on potential strategies. Mobile phones in schools - GOV.UK

4 Responding to incidents

4.1 Policy statement

- *All significant or complex incidents and complaints relating to online safety and unacceptable internet use will be reported to the online safety co-ordinator in the first instance.*

- *Where the incident or complaint relates to a member of staff, the matter must always be referred to the head teacher for action under staff conduct policies for low level incidents or consideration given to contacting the LADO under the CSCP guidance on dealing with allegations against staff where this is appropriate. Incidents involving the head teacher should be reported to the chair of the board of governors.*
- *The school's online safety co-ordinator should keep a log of all online safety incidents and complaints and regularly review the information for*

evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system and use these to update the online safety policy.

- *Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated safeguarding lead, who will make a decision as to whether or not to refer the matter to the police and/or Children's Safeguarding and Family Help in conjunction with the head teacher.*

Although it is intended that online safety strategies and polices should reduce the risk to pupils whilst on-line, this cannot completely rule out the possibility that pupils may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

4.2 Unintentional access of inappropriate websites

- *If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.*

- *Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.*

- *The incident should be reported to the online safety co-ordinator and details of the website address and URL provided.*

- *The online safety co-ordinator should liaise with the network manager or learning platform provider to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.*

4.3 Intentional access of inappropriate websites by a pupil

- *If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).*
- *The incident should be reported to the online safety co-ordinator and details of the website address and URL recorded.*

- *The online safety co-ordinator should liaise with the network manager or learning platform provider to ensure that access to the site is blocked.*

- *The pupil's parents should be notified of the incident and what action will be taken.*

4.4 Inappropriate use of IT by staff

- *If a member of staff witnesses misuse of IT by a colleague, they should report this to the head teacher and the online safety co-ordinator immediately. If the misconduct involves the head teacher or governor, the matter should be reported to the chair of the board of governors.*

- *The online safety co-ordinator will notify the network manager so that the computer, laptop or other device is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the online safety incident report form.*

- *The online safety co-ordinator will arrange with the network manager or learning platform provider to carry out an audit of use to establish which user is responsible and the details of materials accessed.*
- *Once the facts are established, the head teacher will take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate.*

- *If the materials viewed are illegal in nature the head teacher or governor should report the incident to the police and follow their advice, which should also be recorded on the online safety incident report form.*

- *Where incidents raise concerns that the staff member is unsuitable to work with children the matter should also be referred to the LADO under the Schools guidance for managing allegations against staff available on the CSCP schools safeguarding policies webpage.*

4.5 Online bullying

4.5.1 Definition and description

Online bullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Online bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making or sharing derogatory or embarrassing images or videos of someone via mobile phone or email (for example, making or sharing nude and semi-nude images, including AI-generated images where applicable)

Schools should adopt a zero-tolerance approach to child-on-child abuse. Behaviour will never be dismissed as banter, horseplay, part of growing up or boys being boys. All reports will be taken seriously and children affected, including both victims and alleged perpetrators, will receive appropriate support.

Online bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, online bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

4.5.2 Dealing with incidents

The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school. All incidents should be dealt with under the schools' behaviour policies and the *child on child abuse and sexual harassment guidance* available on the CSCP schools safeguarding policies webpage.
School anti-bullying and behaviour policies and acceptable use policies should cover the issue of online bullying and set out clear expectations of behaviour and sanctions for any breach.

- *Any incidents of online bullying should be reported to the online safety co-ordinator who will record the incident on the incident report form and ensure that the incident is dealt with in line with the school's anti-bullying policy. Incidents should be monitored and the information used to inform the development of anti-bullying policies.*

- *Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.*

- *As part of online safety awareness and education, pupils should be told of the "no tolerance" policy for online bullying and encouraged to report any incidents to their teacher.*

- *Pupils should be taught:*
    - *to only give out mobile phone numbers and email addresses to people they trust*
    - *to only allow close friends whom they trust to have access to their social networking page*
    - *not to send or post inappropriate images of themselves*
    - *not to respond to offensive messages*
    - *to report the matter to their parents and teacher immediately.*

- *Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.*

Any action taken on online bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the pupils involved to resolve the issues themselves rather than impose sanctions. This may be facilitated by the School Council or a specialist resource such as Cybermentors.

4.5.3 Action by service providers

All website providers and mobile phone companies are aware of the issue of online bullying and have their own systems in place to deal with problems, such as tracing communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- *Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls. The pupil should also consider changing their phone number.*

- *Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced. The pupil should also consider changing email address.*

- *Where bullying takes place in chat rooms or gaming sites, the pupil should leave the chat room or gaming site immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.*

- *Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.*

- *Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.*

4.5.4 Online bullying of school staff

- *Head teachers should be aware that school staff may become victims of online bullying by pupils and/or their parents. Because of the duty of care owed to staff, head teachers should ensure that staff are able to report incidents in confidence and receive adequate support, including taking any appropriate action against pupils and parents.*

- *The issue of online bullying of school staff should be incorporated into any anti-bullying policies, education programme or discussion with pupils so that they aware of their own responsibilities.*

- *Incidents of online bullying involving school staff should be recorded and monitored by the online safety co-ordinator in the same manner as incidents involving pupils.*

- *Staff should follow the guidance on safe IT use in section 3.4 of this policy and avoid using their own mobile phones or email addresses to contact parents or pupils so that no record of these details becomes available.*

- *Personal contact details for staff should not be posted on the school website or in any other school publication.*

- *Staff should follow the advice above on online bullying of pupils and not reply to messages but report the incident to the head teacher immediately.*

- *Where the bullying is being carried out by parents the head teacher should contact the parent to discuss the issue. A home/school agreement with the parent can be used to ensure responsible use.*

4.6 Harmful sexual behaviour online

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases these actions may be harmful or abusive or may constitute sexual harassment or online bullying and because of the nature of online activities this can lead to more widespread harm and repeat victimisation.

Keeping children safe in education places a duty on schools to respond to any incidents of online sexual harassment such as:

- consensual and non-consensual sharing of nude and semi-nude images or AI generated images
- sexualised online bullying
- unwanted sexualised comments and messages
- sexual exploitation, coercion or threats
- coercing others into sharing images or performing acts online that they are not comfortable with.

Schools should refer to the *Child-on-child abuse and sexual violence and harassment guidance for schools and colleges* available on the CSCP schools safeguarding policies webpage for further details on what actions need to be taken in response to online sexual harassment.

Schools need to make pupils aware that producing and distributing sexual images to peers via the internet or mobile devices may be illegal. Pupils need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

Staff need to be able to react to incidents in a proportional manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised. Guidance for responding to incidents is available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

Schools should also be aware of when any of these behaviours may be linked to extra-familial harm such as the criminal or sexual exploitation of a pupil or is being carried out a gang-related activity. Staff should refer to the CSCP *Extra-familial harm and child exploitation guidance* available on the CSCP website for further details.

4.7 Risk from inappropriate contacts with adults

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met on-line.

School staff should also be aware of pupils being sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records.

- *All concerns around inappropriate contacts should be reported to the online safety co-ordinator and the designated safeguarding lead.*

- *The designated safeguarding lead should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to Children's Safeguarding and Family Help and/or the police.*

- *The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.*

- *The designated safeguarding lead can seek advice on possible courses of action from MASH social workers.*

- *Teachers will advise the pupil on how to terminate the contact and change contact details where necessary to ensure no further contact.*

- *The designated safeguarding lead and the online safety co-ordinator should always notify the pupil's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.*

- *Where inappropriate contacts have taken place using school IT equipment or networks, the online safety co-ordinator should make a note of all actions taken and contact the network manager or learning platform provider to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.*

4.8 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences and may be radicalised as a result of direct contact with online extremists or because they self-radicalise having viewed extremist materials online.

All schools have a duty under the Government's Prevent programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is Camden's Channel Panel, a multi-agency forum that identifies young people who are at risk and develops a support plan to stop the radicalisation process and divert them from extremism.

- *Staff need to be aware of the school's duty under the Prevent programme and be able to recognise any pupil who is being targeted by violent extremists via the internet for the purposes of radicalisation. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.*

- *The school should ensure that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.*

- *All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.*

- *The online safety co-ordinator and the designated safeguarding lead should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.*

- *Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, schools should refer the young person to the MASH. Guidance can be sought from the Prevent Education Manager.*

Further information is available in the CSCP guidance *Safeguarding children and young people from radicalisation and extremism* available on the CSCP website.

4.9 Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- *The school should ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum.*

- *Pastoral support should be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor*

- *Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.*

5 Sanctions for misuse of school IT

Individual schools are responsible for deciding what sanctions will be applied for breach of acceptable use policies. Sanctions applied should reflect the seriousness of the breach and should take into account all other relevant factors. The following is a framework recommended by LGfL that schools may want to adopt: For each point, schools may record their own detailed list of breaches and corresponding sanctions.

5.1 Sanctions for pupils

5.1.1 Category A infringements

These are basically low-level breaches of acceptable use agreements such as:

- *use of non-educational sites during lessons*
- *unauthorised use of email or mobile phones*
- *unauthorised use of prohibited sites for instant messaging or social networking.*

Sanctions could include referral to the class teacher or tutor as well as a referral to the online safety co-ordinator.

School policy

5.1.2 Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of online safety policy that are non-deliberate, such as:

- *continued use of non-educational or prohibited sites during lessons*
- *continued unauthorised use of email, mobile phones or social networking sites during lessons*
- *use of file sharing software*
- *accidentally corrupting or destroying other people's data without notifying staff*
- *accidentally accessing offensive material without notifying staff.*

Sanctions could include:

- *referral to class teacher or tutor*
- *referral to online safety co-ordinator*
- *loss of internet access for a period of time*
- *removal of mobile phone until the end of the day*
- *contacting parents.*

School policy

5.1.3 Category C infringements

These are deliberate actions that either negatively affect school ICT systems or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- *deliberately bypassing security or access*
- *deliberately corrupting or destroying other people's data or violating other's privacy*
- *online bullying*
- *deliberately accessing, sending or distributing offensive or pornographic material*
- *purchasing or ordering items over the internet*
- *transmission of commercial or advertising material.*

Sanctions could include:

- *referral to class teacher or tutor*
- *referral to online safety co-ordinator*
- *referral to head teacher*
- *loss of access to the internet for a period of time*
- *contact with parents*
- *any sanctions agreed under other school policies.*

School policy

5.1.4 Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- *persistent and/or extreme online bullying*
- *deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent*
- *receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act*
- *bringing the school name into disrepute.*

Sanctions could include:

- *referral to head teacher*
- *contact with parents*
- *possible exclusion*
- *removal of equipment*
- *referral to community police officer.*

School policy

5.2 Sanctions for staff

These should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children. Sanctions will be linked to the staff behaviour policy or code of conduct.

5.2.1 Category A infringements

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the head teacher as a low level incident in line with the school's staff conduct policy.

- *excessive use of internet for personal activities not connected to professional development*
- *use of personal data storage media (eg: removable memory sticks) without carrying out virus checks*
- *any behaviour on the world wide web and social media sites such as Twitter that compromises the staff member's professional standing in the school and community, for example inappropriate comments about*

the school, staff or pupils or inappropriate material published on social networking sites
- *sharing or disclosing passwords to others or using other user's passwords*
- *breaching copyright or licence by installing unlicensed software.*

Possible sanctions include referral to the head teacher who will issue a warning.

School policy

5.2.2 Category B infringements

These infringements involve deliberate actions that undermine safety on the internet and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Camden's LADO under the CSCP guidance on dealing with allegations against staff and volunteers available on the CSCP website.

- *serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications*
- *any deliberate attempt to breach data protection or computer security rules, for example hacking*
- *deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent*
- *receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act*
- *bringing the school name into disrepute.*

Possible sanctions include:

- *referral to the head teacher*
- *removal of equipment*
- *referral to Camden's online safety officer*
- *referral to Camden's LADO or the police*
- *suspension pending investigation*
- *disciplinary action in line with school policies.*

School policy

Appendix 1:
Acceptable use policy for primary school pupils

Name:
School:
Class:

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

- *keep my password a secret*
- *only open pages which my teacher has said are okay*
- *tell my teacher if anything makes me feel scared or uncomfortable*
- *make sure all the messages I send are polite*
- *tell my teacher if I get a nasty message*
- *not reply to any nasty message which makes me feel upset or uncomfortable*
- *not give my mobile number, home number or address to anyone who is not a real friend*
- *only email people I know or if my teacher agrees*
- *only use my school email address*
- *talk to my teacher before using anything on the internet*
- *not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school)*

- *not load photographs of myself onto the computer*
- *never agree to meet a stranger.*

Parents

□ *I have read the above school rules for responsible internet use and agree that my child may have access to the internet at school. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.*

□ *I agree that my child's work can be published on the school website.*

□ *I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published.*

Signed:
Date:

Appendix 2:
Acceptable use policy for secondary school pupils

Name:
School:
Class:

I understand that all computer equipment is owned by the school and that I can use the internet at school as long as I behave in a responsible way that keeps me and others safe. I also understand that the school ICT system is monitored and that if I do not follow the rules, I may not be allowed to use the school computers.

I will:

- *only use the school's computers for school work and homework*
- *only delete my own files and not look at other people's files without their permission*
- *keep my login and password safe and not let anyone else use it or use other people's login or password*
- *not bring in files to school without permission*
- *ask a member of staff for permission before using the internet*
- *not visit websites I know are banned by the school or use non-school email accounts or social networking sites*
- *only email people I know or whom my teacher has approved*
- *make sure any messages I send or information I upload is polite and sensible*
- *not open attachments or download files unless I have permission or I know and trust the person who sent it*

- *not give out my home address, phone numbers or send photographs or videos or give any other personal information that may identify me, my family or my friends unless my teacher has given permission*
- *never arrange to meet someone I have only met on-line unless my parent, carer or teacher has given me permission and I will take a responsible adult with me*
- *tell my teacher or responsible adult if I see anything I am unhappy with or receive a message I do not like and I will not respond to any bullying messages*
- *only use my mobile phone or other device in school when I have permission*
- *not use any internet system to send anonymous or bullying messages or to forward chain letters*
- *log out when I have finished using the computer.*

Signed:
Date:

Parents

□ *I have read the above school rules for responsible internet use and agree that my child may have access to the internet at school. I understand that the school will take all reasonable precautions to ensure pupils do not have access to inappropriate websites, and that the school cannot be held responsible if pupils do access inappropriate websites.*

□ *I agree that my child's work can be published on the school website.*

□ *I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published.*

Signed:
Date:

Appendix 3

Acceptable use policy for staff and governors

Access and professional use

- *All computer networks and systems belong to the school and are made available to staff and governors for educational, professional, administrative and governance purposes only.*
- *Staff and governors are expected to abide by all school online safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken against staff or governors being removed.*
- *The school reserves the right to monitor internet activity and examine and delete files from the school's system.*
- *Staff and governors have a responsibility to safeguard pupils in their use of the internet and reporting all online safety concerns to the online safety co-ordinator.*
- *Copyright and intellectual property rights in relation to materials used from the internet must be respected.*
- *E-mails and other written communications must be carefully written and polite in tone and nature.*
- *Anonymous messages and the forwarding of chain letters are not permitted.*
- *Staff and governors will have access to the internet as agreed by the school but will take care not to allow pupils to use their logon to search the internet.*
- *Staff and governors will follow good practice advice at all times and will ensure online activity meets the standards expected of professional conduct.*

Data protection and system security

- *Staff and governors should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand.*

- *Use of any portable media storage devices is permitted where virus checks can be implemented on the school ICT system using appropriate software. Portable media should be encrypted to reduce the risk of breach of the GDPR and the Data Protection Act 2018.*

- *Where staff are accessing cloud-based school systems (eg; Teams, CPOMS, Bromcom) via personal devices such as mobile phones they should:*

    - *Use either a 2 factor authentication or 6 digit passcode **and***
    - *Delete anything they download from their personal devices as soon as it is no longer required.*
- *Downloading executable files or unapproved system utilities will not be allowed and all files held on the school ICT system will be regularly checked.*

- *Staff and governors will not allow others to access their individual accounts. Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.*

- *Files should be saved, stored and deleted in line with the school policy.*

- *Care will be taken to check copyright and not publish or distribute others' work without seeking permission.*

Personal use

- *Staff and governors should not browse, download or send material that could be considered offensive to colleagues and pupils or is illegal.*

- *Staff and governors should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any computers or hardware used at home safe.*

- *Staff and governors should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute.*

- *School ICT systems may not be used for private purposes without permission from the head teacher.*

- *Use of school ICT systems for financial gain, gambling, political purposes or advertising is not permitted.*

I have read the above policy and agree to abide by its terms.

Name:
School:
Signed:
Date: