

St Alban's C.E Primary School



Online safety policy

September 2026

Amendments shown in dark blue

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	37
Appendix 2: Acceptable use policies for secondary schools	38
Appendix 3: Acceptable use policies for staff	

Key contacts

School

Name of school: St Alban's CE Primary School

Headteacher

Name: Rebecca Harris

Contact details: head@stalbans.camden.sch.uk

Deputy designated safeguarding lead

Name: Sarah Maltese

Contact details: via the school office

Online safety co-ordinator:

Name: Rebecca Harris

Contact details: head@stalbans.camden.sch.uk

Nominated LGfL contact:

Name: Rebecca Harris

Contact details: head@stalbans.camden.sch.uk

IT systems/Data manager:

Name: Ebrahim Ali

Contact details: support@camdensitss.org.uk

Designated safeguarding lead:

Name: Rebecca Harris

Contact details: head@stalbans.camden.sch.uk

Nominated online safety/safeguarding governor:

To be confirmed by the governing body

Contact details: via the school office

London Borough of Camden

Camden Safeguarding Children Partnership (CSCP):

Advice and partnership enquiries

Contact: 020 7974 8752 | CSCP@camden.gov.uk

Local Authority Designated Officer (LADO):

Camden LADO

Contact: 020 7974 4556

Email: LADO@camden.gov.uk

Children and Families Contact Service (including MASH):

Duty manager
Tel: 020 7974 3317 | Out of hours: 020 7974 4444
Email: LBCMASHadmin@camden.gov.uk

Camden Prevent Team / Channel advice

Email: prevent@camden.gov.uk
Tel: 020 7974 1008

1 Information on internet technology

1.1 Introduction

The educational and social benefits of technology should be promoted while children are safeguarded from online harm. The school will teach pupils how to use technology safely, respectfully, critically and responsibly, and how to seek help when something worries them.

This policy sets out St Alban's whole-school approach to online safety, including education, professional conduct, data protection, filtering and monitoring, incident response and partnership with parents and carers.

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.

KCSIE 2026 groups online safety risks into four interrelated categories: content, contact, conduct and commerce.

1.2.1 Content

Content risk includes exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, antisemitism, self-harm, suicide, radicalisation, extremism, extreme violence, misinformation, disinformation and conspiracy theories. Content may be created or altered using AI.

1.2.2 Contact

Contact risk includes harmful interaction with other users or generative-AI applications that simulate people. This includes peer pressure, commercial advertising and adults posing as children in order to groom or exploit them for sexual, criminal, financial or other purposes.

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.

Technology may also facilitate child-on-child abuse, online bullying, harassment and exploitation. See sections 4.5 to 4.7.

1.2.3 Commerce

Commerce risk includes online gambling, inappropriate advertising, phishing, scams, fraud, identity theft and pressure to make purchases or reveal financial or account information.

1.2.4 Conduct

Conduct risk concerns online behaviour that increases the likelihood of, or causes, harm. Pupils may place themselves or others at risk by:

- creating, accessing or sharing illegal, inappropriate, abusive or discriminatory content
- using online information or AI-generated material in a way that breaches copyright or intellectual property rights
- sharing personal information, images or location data without understanding the audience, permanence or possible misuse
- engaging in online bullying, harassment or child-on-child abuse (see section 4.5)
- making, sharing or manipulating nudes or semi-nudes, including AI-generated 'deepfakes' or 'deep nudes'; all such incidents involving children require a safeguarding response.

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 understand that technology is a significant component in many safeguarding and wellbeing issues and may facilitate abuse, neglect and exploitation online and offline, including 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.
- This policy will be reviewed at least annually and whenever a safeguarding risk, significant incident, new technology (including generative AI), system change or relevant national guidance requires an earlier review.

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>

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 filtering and monitoring systems that meet the Department for Education's current core standard and cover school-managed devices, networks, relevant locations and, where technically possible, dynamic, personalised and AI-generated content.

[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 \(lgfl.net\)](#)

- 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

Online safety is a whole-school responsibility. The governing body has strategic oversight; the Headteacher and senior leadership team oversee implementation; the DSL leads on safeguarding and online safety; IT support manages technical provision; and every member of staff must understand, follow and act on the school's procedures.

2.3.1 Headteacher's role

The Headteacher has overall responsibility for online safety 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 Headteacher 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.

The governing body must receive assurance that filtering and monitoring standards are met. A recorded review will take place at least once each academic year, led by senior leaders with the DSL and IT support and involving the responsible governor. Additional checks and reviews will follow relevant incidents, system changes or the introduction of new technology such as generative AI.

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 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 Headteacher, DSL, IT support and nominated governor; check relevant reports; respond to safeguarding concerns; and ensure that filtering and monitoring decisions, checks, exceptions and actions are recorded and reviewed*
- *assess the benefits and risks of emerging technology, including teacher-facing and pupil-facing generative AI, with the DSL, IT support and relevant data-protection advice*
- *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.*

The online safety co-ordinator and DSL will receive appropriate, up-to-date training. Staff training will reflect KCSIE 2026, local safeguarding arrangements and changes in technology and online harms.

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 Headteacher 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

Online incidents with safeguarding implications must be referred immediately to the DSL or deputy, who will take prompt action under the child protection policy and KCSIE 2026, including referral to the Children and Families Contact Service and/or police where required.

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. The CSCP online safety leaflet for parents should also be available on the school website: <https://cscp.org.uk/parents-and-carers/online-safety/>

The Headteacher, board of governors and the online safety coordinator should consider what strategies to adopt in order 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 school systems will use individual accounts wherever possible, with permissions limited to the user's role. Visitors requiring access must be authorised and use an appropriately restricted account.*
- IT support will maintain an accurate record of user accounts and access rights. Accounts must not be shared and must be amended or disabled promptly when roles change or users leave.*
- Passwords or passphrases must be strong, unique and protected. They must be changed immediately if compromise is known or suspected; routine forced changes are not required solely because time has passed. Multi-factor authentication must be enabled for staff cloud-service and remote-access accounts.*
- 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

- Personal data will be processed in accordance with the Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025. Information will be stored securely, with access limited to those who need it for an authorised purpose.*
- Personal data shared with other organisations will use an approved secure method. Suspected personal-data breaches must be reported immediately to the Headteacher and the school's data-protection contact so that containment, assessment, recording and any required notification can occur promptly.*

- *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).*
- *Appendix 2 is a Camden model for secondary settings and is not used by this primary school.*
- *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 Headteacher 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 in order 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 will reinforce the school's mobile phone-free expectations: pupils must not access mobile phones or other included smart technology during the school day except where an individual exception has been approved.*

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.

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 staff and governors will receive appropriate online-safety information or training at induction and regular updates thereafter. Staff safeguarding training will include their roles and responsibilities for filtering and monitoring, how to report concerns and how emerging technology, including AI, may create risk.*
- *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.*

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 for further guidance.

[Model-Schools-Social-Media-Policy-2020.docx \(live.com\)](#)

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.*
- Images or recordings of pupils may be made only on school-approved equipment for an authorised educational purpose. Personal phones, cameras, accounts or storage must never be used.*
- 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.*
- *Personal data must be stored only in approved school systems. Staff must not download or transfer pupil information to personal devices or unapproved storage.*
- *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 or change role, their line manager and IT support will recover school equipment, update access rights and disable accounts promptly. School information must be transferred or retained in accordance with the school's retention and security procedures.

3.6 Safe use of technology

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 pupils will be supervised at a level appropriate to their age, needs, activity and understanding whenever they use online services.*
- *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.*
- *Any temporary filtering exception for an educational purpose must be authorised, risk assessed, recorded, time limited and removed when no*

longer required. Filtering must not unreasonably restrict teaching and learning.

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 Headteacher, 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.*
- *In order 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 a remote lesson only where there is a clear approved purpose, a lawful basis, appropriate safeguards and prior communication with those involved*
- *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 Headteacher, 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.*
- *Photographs or videos of pupils will be used only for a specified, lawful and transparent purpose. Where consent is the lawful basis, valid consent will be obtained and withdrawal respected.*
- *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 will be stored only in approved secure school systems and unnecessary copies will be deleted.*
- *Images will be labelled, retained and deleted in accordance with the school's data-retention schedule, privacy information, consent arrangements and safeguarding requirements.*
- *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

St Alban's is a mobile phone-free environment by default. Pupils must not access mobile phones or other included smart technology at any point during the school day, including lessons, transitions, breaktimes and lunchtime, except where an individual exception has been approved.

Any device brought to school must be switched off and stored in the manner specified by the school. Parents should contact the school office if they need to communicate urgently with their child.

Exceptions may be agreed by the Headteacher where necessary and proportionate, for example to support a medical need, disability or special educational need, or another exceptional circumstance. The arrangement and safeguards will be recorded and reviewed.

Pupils may use only school-managed devices and approved services unless the Headteacher has expressly authorised another arrangement. All use remains subject to the school's acceptable-use, filtering and monitoring requirements.

Staff personal phones and smart devices must be kept out of sight and not used in front of pupils, except for an approved professional purpose or emergency. Personal devices must never be used to photograph, film or record pupils.

A device may be confiscated, searched or retained only in accordance with the behaviour policy and current DfE searching, screening and confiscation guidance. Where nudes or semi-nudes may be involved, staff must not view, copy, print, forward or ask a child to share the image; the device must be secured and the DSL consulted immediately.

The school will follow current DfE advice on searching, screening and confiscation and the UKCIS advice on sharing nudes and semi-nudes.

This section reflects the statutory Mobile phones in schools guidance, effective from 1 September 2026, and should be read with the school's Behaviour Policy.

Approved exceptions and storage or collection arrangements are recorded and communicated.

4 Responding to incidents

4.1 Policy statement

- *All significant, complex or safeguarding-related online incidents and complaints must be reported promptly to the online safety co-ordinator and DSL. Immediate danger or suspected crime must be escalated without delay.*

- *Concerns about staff conduct must be reported to the Headteacher under the staff code of conduct and child protection procedures. The Headteacher will consider the harm threshold, low-level concerns procedures and consultation with the LADO. Concerns about the Headteacher must be reported to the Chair 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.*
- *The DSL will respond to online safeguarding concerns under KCSIE 2026 and the child protection policy, including referral to the Children and Families Contact Service and/or police where required.*

Although it is intended that online safety strategies and policies 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 accidentally 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

- *Misuse of technology by a member of staff must be reported immediately to the Headteacher. Concerns about the Headteacher must be reported to the Chair of Governors. Safeguarding evidence must be preserved without unnecessary access, copying or investigation by unqualified staff.*
- *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 Headteacher will take any necessary disciplinary action against the staff member and report the matter to the school governors and the police where appropriate. Where appropriate, consideration should be given to contacting the LADO for advice.*
- *If the materials viewed are illegal in nature the Headteacher 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.*

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, sexting/"happy slapping").

Online bullying may affect pupils or staff and can occur through many services, including messaging, social media, gaming and AI-generated or manipulated content. Serious conduct may constitute an offence under the Protection from Harassment Act 1997, Malicious Communications Act 1988 or Communications Act 2003.

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 guidance. [Child-on-child-abuse-and-sexual-violence-guidance.pdf \(cscp.org.uk\)](https://www.cscpschools.org.uk/child-on-child-abuse-and-sexual-violence-guidance.pdf)

- *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

- *Headteachers 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, Headteachers 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 are 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 Headteacher immediately.*
- Where the bullying is being carried out by parents the Headteacher 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

Online sexual harassment and harmful sexual behaviour may involve messages, livestreams, photographs, videos, manipulated images or wholly AI-generated material. It can cause repeated and widespread harm and must never be dismissed as banter, an inevitable part of growing up or 'just online'.

Under KCSIE 2026, all incidents involving the making or sharing of nudes or semi-nudes require a safeguarding response, including:

- consensual or non-consensual making or sharing of nudes or semi-nudes*
- sexualised online bullying*
- unwanted sexualised comments and messages*
- sexual exploitation, coercion or threats*
- coercing or pressuring others to share images or perform acts online, including financial or sexual extortion*

Staff must report concerns immediately to the DSL and follow KCSIE 2026, the child protection policy and the UKCIS 'Sharing nudes and semi-nudes' advice. Staff must not view, copy, print, forward or delete images themselves.

<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>

Pupils will be taught, in an age-appropriate way, that making, possessing or sharing indecent images of a person under 18 may be illegal; that images can be copied and redistributed; and that manipulated and AI-generated images can be equally harmful and may also be illegal.

The DSL will use professional judgement and a proportionate, child-centred response, prioritising welfare and avoiding unnecessary criminalisation while referring to children's social care and/or police whenever harm, immediate risk, adult involvement, coercion or other aggravating factors require it.

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* for further details.

[CSCP-extra-familial-harm-and-child-exploitation-guidance.pdf](#)

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.*

- *Parents or carers should normally be informed early and involved in supporting the child, unless doing so may place the child at risk or prejudice an investigation. Any decision not to inform them must be made and recorded by the DSL with appropriate advice.*
- *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 at: <https://cscp.org.uk/resources/radicalisation-and-extremism-resources/>

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

Record the incident, reteach expectations and use a proportionate warning or restorative response; inform parents as appropriate.

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

Record and refer to the Headteacher or online-safety co-ordinator; consider temporary access restriction and inform parents.

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 Headteacher*
- *loss of access to the internet for a period of time*
- *contact with parents*
- *any sanctions agreed under other school policies.*

School policy

The Headteacher and DSL will review; apply behaviour and safeguarding procedures; restrict access or equipment and seek advice as required.

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 Headteacher*
- *contact with parents*
- *suspension or permanent exclusion only where the statutory threshold and the school's Exclusion Policy are met*
- *removal of equipment*
- *referral to community police officer*
- *referral to Camden's online safety officer.*

School policy

Escalate immediately to the Headteacher and DSL; preserve evidence; consider exclusion, suspension or agency referral under 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 that may amount to misconduct and will be addressed by the Headteacher under the staff code of conduct and disciplinary procedures. Any safeguarding element will be considered under the low-level concerns or allegations procedures as appropriate.

- *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 Headteacher who will issue a warning.

School policy

The Headteacher will record and review; consider support, retraining, a warning, access restriction and low-level-concern procedures.

5.2.2 Category B infringements

These are serious or deliberate actions that undermine safety, security, data protection or professional boundaries and may amount to gross misconduct or raise suitability concerns. The Headteacher will follow disciplinary and safeguarding procedures and consult the LADO and/or police where appropriate.

- *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 Headteacher*
- *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

Report to the Headteacher or DSL (or Chair if about the Headteacher); preserve evidence and follow disciplinary, safeguarding, LADO and police procedures.

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 account or another account my teacher has approved*
- *only use websites, apps or AI tools that my teacher has approved and follow their instructions*
- *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:

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 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.*
- *Use of school systems may be logged and reviewed by authorised staff for safeguarding, security and operational purposes in accordance with the law, school policies and privacy notices.*
- *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

- *Personal data must be sent, accessed and stored only through approved secure systems. Staff and governors must not download or transfer school information to personal devices or unapproved storage.*

- *Only school-approved encrypted portable storage may be used, following required malware-checking and secure-handling procedures.*
- *When accessing approved cloud-based school systems, staff and governors must:*
 - *use multi-factor authentication and secure the device with an appropriate passcode, password or biometric control*
 - *avoid downloading personal data; where an approved download is necessary, delete it securely as soon as the authorised purpose ends.*
- *Downloading executable files or unapproved system utilities will not be allowed and all files held on the school ICT system will be regularly checked.*
- *Accounts and credentials must not be shared. Users must use strong, unique passwords or passphrases, keep multi-factor authentication secure, lock unattended devices and report suspected compromise immediately.*
- *Files should be saved, stored and deleted in line with the school policy.*
- *Copyright and intellectual property must be respected, including when using AI-generated content or pupils' original work. Permission or another lawful basis is required before protected work is uploaded, reused or distributed.*
- *Generative AI may be used only for an approved purpose. Personal, confidential or safeguarding information must not be entered into an AI tool unless the school has approved both the tool and the specific use. Users remain accountable for accuracy, bias, suitability, safeguarding and copyright.*

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 Headteacher.*
- *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:

