



Online Safety Policy

Statement of policy intent

London Christian School (LCS) is committed to providing access to educationally beneficial digital technologies whilst responsibly monitoring access and educating pupils, parents and staff in internet safety. Internet (aka online) safety is a significant part of the school's wider safeguarding and anti-bullying strategies. In compliance with KCSIE 2025, guidance from the UK Safer Internet Centre, the Prevent strategy 2015 and other statutory documents, this is the statement of general policy and arrangements to protect, educate and build resilience and responsibility when using the Internet, and all other digital devices at LCS. We want all our children to be safe cyber citizens, who make a positive contribution in this increasingly digital age.

This policy is part of the school's statutory safeguarding strategy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

NOTE: this policy builds on the London Grid for Learning (LGfL) and The School Bus exemplary policy and takes into account advice and best practice as the result of using the Southwest Grid for Learning (SWGfL) School Online Safety Self Review Tool; 360 ° SAFE.

Contents

1. Introduction and Overview

- Legal framework
- Aims
- Risks
- Scope
- The technologies in our school
- Roles and responsibilities
- Communication of this policy

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent/carer awareness and training

3. Handling safeguarding concerns and incidents

- Sharing nudes and semi-nudes
- Upskirting
- Cyberbullying
- Child-on-child sexual violence and sexual harassment
- Misuse of school technology
- Extremism
- Data protection and cyber security
- Appropriate filtering and monitoring
- Use of artificial intelligence

4. Data Protection and Security

- Passwords
- CCTV and walkie-talkies
- Network management (user access, backup, protocols etc.)
- Equipment disposal and data deletion
- Cloud platforms

5. Electronic Communications

- Email
- School website
- Digital images and videos

6. Social Media

- Staff, pupils and parents social media presence

7. Device Usage

- Storage, syncing and access on school owned digital devices
- Handling hardware around the school
- Personal devices for staff
- Personal devices for pupils
- Personal devices for parents
- Personal devices for volunteers, contractors and governors
- Trips/events away from school

Appendices

- Appendix A- Roles
- Appendix B- Key Stage 1 Acceptable Use Agreement
- Appendix C- Key Stage 2 Acceptable Use Agreement
- Appendix D- EYFS Acceptable Use Agreement
- Appendix E- Staff and Governor Acceptable Use Agreement
- Appendix F- Guidance for Parents, Visitors & Contractors
- Appendix G- How specific infringements will be handled – Sanctions etc.
- Appendix H- Example of letter sent to parents if inappropriate material

1. Introduction and Overview

Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children safe in education 2025'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct

- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Prevent Duty Policy
- Artificial Intelligence Policy

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out key principles and expectations for all members of the LCS community with respect to their online behavior, attitudes and activities, and the use of IT-based technologies (including when devices are offline)
- Helping safeguarding and senior leadership to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues, curriculum leads and beyond.
- Facilitating the safe, responsible and respectful use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - For the protection and benefit of the children and young people in their care,
 - For their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice, and
 - For the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.

Risks

We aim to minimise risk at all times. KCSIE (2025) summarises risks under four different categories. This is reflected in the main areas of risk we have listed for our school community below:

- **Content:** Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.
- **Contact:** The school will educate pupils about the potential dangers of interacting with others online. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.
- **Conduct:** Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with creating, sharing, or receiving explicit images, including both consensual and non-consensual exchanges of nudes and semi-nudes. Online bullying, including the use of social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.
- **Commerce:** The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when

confronted with suspicious online activity.

Scope

This policy applies to all members of the LCS community (including teaching, supply and support staff, governors, pupils, volunteers, parents/carers, visitors, contractors and community users) who have access to our digital technology, networks and systems, whether on site or remotely, and at any time, or who use technology in their school role.

The technologies in our school

We use a range of technologies at LCS that reflects the all-encompassing role that ICT has in our modern lives. Current and exciting, new technologies are used in school and, just as importantly, outside of school.

These include:

- The Internet; a variety of Internet services are used
- The World Wide Web
- Email
- Blogs
- Social networks
- Video broadcasting sites
- Gaming sites
- Virtual learning environments
- Google Suite for education
- iPads – managed through Apple School Manager and Mosyle MDM (Mobile Device Management)
- Chromebooks – managed through Google Workspace Admin console
- School Apple Smartphones managed through Apple School Manager and Mosyle MDM (Mobile Device Management), while school Android smartphones managed through Google Workspace Admin console
- iPod touches with email, web functionality, managed through Apple School Manager and Mosyle MDM (Mobile Device Management)
- School computers managed through school Active Directory and Domain Services installed on school servers
- Lego WeDo Robotic kits
- Interactive WhiteBoards
- Cameras
- Microphones
- Beebots
- RM Integr8
- CCTV
- Walkie talkies
- BBC Micro:bit

Roles and Responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the school community should read the relevant section in Appendix A of this document that describes individual roles and responsibilities. Please note there is one for 'All Staff' which must be read even by those who have a named role in another section. All staff have a key role to play in feeding back on potential issues.

Communication of this policy

This policy is a regularly updated, living document. Reviews of this online safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement. This policy and associated

Acceptable use Policies will be communicated to all stakeholders in the following ways:

- Posted on the school website
- Part of school induction pack for all new staff and governors (including temporary, supply and those starting mid-year)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school

This policy will be summarised in bullet point form using accessible language appropriate to volunteers/contractors to form an Acceptable Use Agreement, and must be read and agreed on entry to the school. The documents will also be available in full on the school website, and volunteers/contractors will be encouraged to read this before entry.

2. Education and curriculum

Pupil online safety curriculum

The Internet and digital devices provide many benefits but they also can create risks and dangers that we want our children to be aware of. So that our pupils can grow into independent, responsible, safe cyber citizens, LCS takes a whole school approach to online safety through its technical infrastructure, physical monitoring, staff supervision, training for pupils and management of personal data. At LCS, we recognise that online safety and broader digital resilience must be threaded throughout the curriculum, thus we refer to the cross-curricular framework '[Education for a Connected World](#)' from UKCCIS to inform our planning, as well as the document '[Teaching Online Safety in Schools](#)'.

The following subjects have the clearest online safety links (see relevant role descriptors above for more information):

- PSHE
- Relationships Education, Relationships and Sex Education (RSE) and health
- Computing
- Citizenship

Below are some specific examples of how we teach online safety, however, as stated in the role descriptors and paragraphs above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

This school:

- Has a clear, progressive online safety education programme (informed by other outside agencies such as South West Grid for Learning and 'Education for a Connected World' from UKCCIS) as part of the Computing curriculum, and this also links with PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to the children's age and experience
- Plans the use of technology (devices, the internet, social media, new technology such as augmented reality, etc) carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind students about their responsibilities through the Pupil Acceptable Use Policies
- Ensures all staff encourage sensible use of technology, monitoring what pupils/students are doing and considering potential dangers and the age appropriateness of websites
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights
- Ensures pupils only use school-approved systems and publish within appropriately secure/age-appropriate environments
- All staff carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with

search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law

- Reviews the curriculum (including for SEND pupils) enabling us to weave in self-image and identity, online relationships, online reputation, online bullying, managing online information, health, wellbeing and lifestyle, privacy and security, and copyright and ownership

Staff and governor training

This school:

- Makes regular training available to staff and governors on online safety issues and the school's online safety education program. Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.
- Provides, as part of the induction process, all new staff and governors, including those on university/college placement and work experience, with information and guidance on the Online Safety Policy and the school's Acceptable Use Policies

Parent/carers awareness and training

This school:

- Provides guidance and training for parents
- Gives parents/carers extra resources through the school portal, on the school website and through Digital Tips in weekly newsletters

3. Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all staff should speak to the DSL with any concerns (no matter how small these seem) to contribute to the overall picture or highlight what might not yet be a problem.

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cyber Security

This school commits to take all reasonable precautions to safeguard pupils online but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the Designated Safeguarding Lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on

My Concern- this includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

Any concern/allegation about staff misuse is always (similar to any safeguarding allegation) referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance [Behaviour in Schools, advice for headteachers and school staff September 2024](#) provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 31-33 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The school should ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

For more information on reporting channels for online safety concerns, please visit reporting.lgfl.net.

The following sub-sections provide detail on managing particular types of concern.

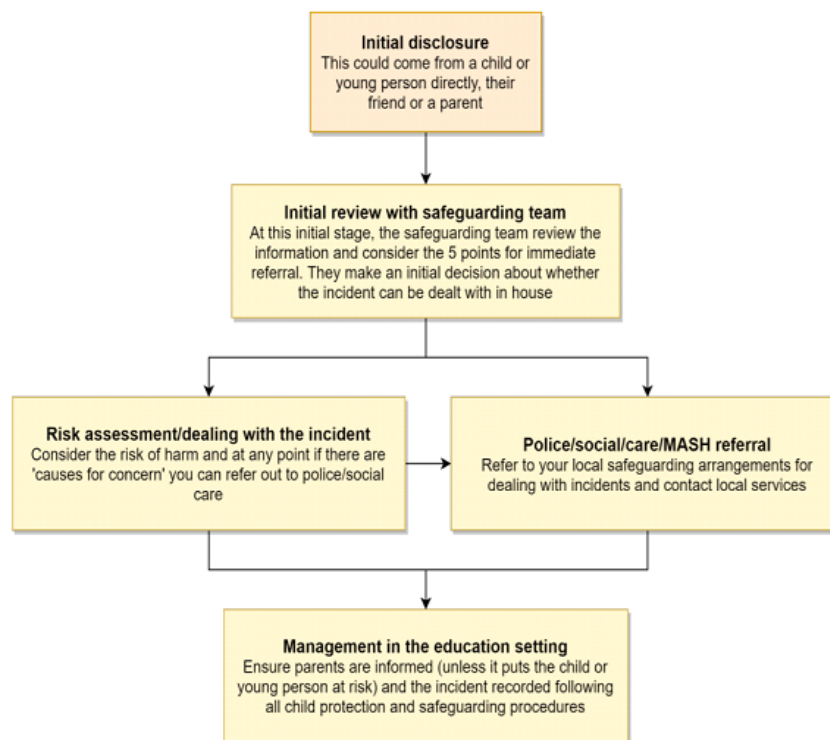
Nudes – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as [Sharing nudes and semi-nudes: advice for education settings](#).

There is a one-page overview called [Sharing nudes and semi-nudes: how to respond to an incident](#) for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. **Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.**

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will use the full guidance document, [Sharing nudes and semi-nudes – advice for educational settings](#) to decide next steps and whether other agencies need to be involved (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils.



The following LGfL document (available at nudes.lgfl.net) may also be helpful for DSLs in making their decision about whether to refer a concern about sharing of nudes:

SAFEGUARDING QUESTION TIME

Q: WHEN SHOULD WE REFER NUDE SHARING?

A: IMMEDIATELY *IF* THE IMAGE/VIDEO:

- involves an adult
- is potentially coerced, blackmailed or groomed or concerns about capacity to consent
- might depict sexual acts unusual for their developmental stage or violent
- involves sexual acts / under 13s
- or the young person is at immediate risk of harm..., suicidal or self-harming



Text simplified, taken from page 20 of 'Sharing Nudes and Semi-Nudes', UKCIS – search.gov.uk

"We recommend DSLs read the entire UKCIS document; there is much more to know than this, and many helpful resources including training, scenarios and further guidance. Note also the one-pager for all staff!"

Priority Areas

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Cyberbullying

Cyberbullying (which may also be referred to as online bullying), including incidents that take place outside of school should be treated like any other form of bullying and the school bullying policy should be followed. This includes issues arising from banter. Please see our school [Anti-Bullying Policy](#).

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Data protection and cyber security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policy. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2025, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's '[Filtering and monitoring standards for schools and colleges](#)'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. Mike Burden is the named governor with responsibility for filtering and monitoring.

LCS is following the new DfE filtering and monitoring standards, which requires us to: -identify

and assign roles and responsibilities to manage filtering and monitoring systems -review

filtering and monitoring provision at least annually

-block harmful and inappropriate content without unreasonably impacting teaching and learning

-have effective monitoring strategies in place that meet their safeguarding needs

ALL STAFF need to play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via email to the DSL.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out. It is very important that schools understand the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems. There are guidance videos and flyers to help with this at <https://safefiltering.lgfl.net> and training is provided for all staff / safeguarding teams / technical teams as appropriate.

At London Christian School:

-web filtering is provided by Surf Protect Quantum on school site

-changes can be made by Krzysztof Jurek, Faye Martin, Katie Vivyan, Nicola Collett-White and Stephen Lowries

-overall responsibility is held by the DSL with support from the head teacher

-technical support and advice, setup and configuration are from Hextrio, Krzysztof Jurek

-regular checks are made half termly by the DSL to ensure filtering is still active and functioning everywhere. These are evidenced in weekly safeguarding meeting minutes with the headteacher.

-an annual review is carried out as part of the online safety audit to ensure a whole school approach (a template is available at onlinesafetyaudit.lgfl.net]

According to the DfE standards, “a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

NOTE: LCS will take all reasonable precautions to ensure online safety and minimise risk. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on an LCS computer or mobile device. This policy puts procedures in place should such material appear.

Use of Artificial Intelligence

Please see the school Artificial Intelligence Policy.

4. Data Protection and Security

There are references to the relationship between data protection and safeguarding in KCSIE 2024 and ‘Data protection: a toolkit for schools’ (April 2018), which the DPO and DSL seek to apply. We are aware that ‘GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.’

All pupils, staff, governors, volunteers, contractors and parents are bound by the school’s data protection policy and agreements. Further, this school makes use of the many helpful GDPR resources e.g. GDPR.co.uk, School Bus.

Rigorous controls on our school network, USO sign-on, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: Egress, GSuite for Ed Admin Console, Mosyle, Centrastage, Jungle Disk, Amazon S3 and Sophos Intercept X

The Head Teacher/DPO and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. We use [DfE approved systems](#) to send ‘protect-level’ (sensitive personal) data over the Internet; but if no secure file transfer solution is available, and email is used, then the data / file must be protected with security encryption. Sensitive data is kept onsite or backed up externally using encryption. Where none of these options is available, the DPO and DSL should be informed in advance.

Passwords

- This school makes it clear that staff and pupils must always keep their passwords private, and must not share with others; if a password is compromised the school should be notified immediately. ● All pupils have their own unique username and private passwords. We teach children what a strong password looks like and why passwords need to be non-guessable but memorable to the user. ● All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use strong passwords and teach this.
- Passwords are automatically changed throughout the year via Google Admin, with good passwords only accepted as replacements, and our technician also sends out password changes for Windows logins too.

- Our DPO also sends out reminders throughout the year to keep passwords safe.

CCTV and walkie-talkies

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. .
- When using walkie-talkies as a school, staff are discrete and never communicate any personal information (e.g. only first names of children are used, not surnames).

Network management (user access, backup, protocols etc.)

To ensure the network is used safely, this school:

- Ensures staff read and signs the school's online safety policy and relevant AUPS
- Ensures online access to the server is through a unique, audited username and password
- Ensures strict supervision is in place if a short term visitor must access the wifi on their device
- Ensures all pupils have their own unique username and password for logging into certain cloud services. Children use a shared log in for the Chromebooks. We have small class sizes and screens are visible to teachers in small classroom environments
- Makes clear that no one should log on as another user, other than the one we tell them, and makes clear that pupils should never be allowed to log-on or use teacher and staff logins
- Has set-up the network with a shared work area for pupils and for staff. Staff and pupils are shown how to save work and access work from these areas
- Staff have a secure area(s) on the network to store sensitive files
- Requires all users to log off when they have finished working or are leaving the computer unattended ● Ensures all equipment owned by the school and/or connected to the network has up to date virus protection
- Maintains equipment to ensure health and safety is followed
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems: G Suite for Education
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is only through approved systems
- Has a clear disaster recovery system in place that includes a secure, remote offsite backup of data ● Ensures that all 'Protect level' data sent over the Internet is encrypted or only sent within the approved secure system in our school
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting up applications and Internet web sites with additional monitoring/auditing software available through facilities such as Google admin
- Has daily backup of specific school data and uses secure, 'Cloud' storage for data backup that conforms to DfE guidance
- All servers are in lockable locations and managed by DBS-checked staff
- All IT and communications systems installed professionally and regularly reviewed by a technical team who are kept up to date with relevant services and policies, to ensure they meet health and safety standards

Equipment disposal and data deletion

- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

Cloud platforms

- This school adheres to the principles of the Department for Education document '[Cloud computing](#)

[services: guidance for school leaders, school staff and governing bodies](#)'.

- We consider Data Protection implications before adopting new cloud platforms, and check for GDPR compliance e.g. Data Protection policy .
- Privacy statements inform parents when and what sort of data is stored in the cloud.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such.
- Pupils and staff are only given access and/or sharing rights as appropriate and when they can demonstrate an understanding of what data may be stored and how it can be seen.
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain).

6. Electronic Communications

This section only covers electronic communications.

Email:

- Staff at this school use Gmail accounts as part of our GSuite for education package

General principles for email use are as follows:

- Emailing in school between pupils and teachers happens for a number of reasons e.g. chat functionality to enable homework hand-ins in Google Classroom, as a Homework submission tool, to aid learning how to email, contributing to our VLE
- Under normal circumstances, email is the only means of electronic communication to be used between staff and pupils/parents (in both directions) and use of a different platform in any other circumstance must be approved in advance by the DPO in advance. In a lock down emergency or on a school trip communication may take place through other means (see 'Trips/Events away from school' below)
- Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Head Teacher (if by a staff member)
- Emailing between teacher and pupil/parent may only take place using the email systems named above. There should be no circumstances where a private email account is used; if this happens by mistake, the DSL/Head Teacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately
- Pupils in Year 1-6 are restricted to emailing within the school and cannot email external accounts
- When using email, appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils and staff are not allowed to use the email systems for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination
- Staff or pupil personal data should never be sent/shared/stored on email:
 - If data needs to be shared with external agencies we use DfE approved systems including DfE S2S
 - If Protect-level' data must be transferred by email, because no secure file transfer solution available for the situation, then the data/file must be protected with security encryption
 - Internally, staff should use the school network, including when working from home when remote access is available via our GSuite, which is password protected and enables one to remotely work within the cloud without any need to download data.

See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective parents) with a key reputational value. The Head Teacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. Management of the website day-to-day is delegated to the headteacher for the short term. Innermedia hosts the site.

Where other staff submit information for the website, they are asked to remember:

- The school website complies with the Education (Independent School Standards) Regulations 2014
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- Photographs/videos published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

Digital images and video

- We gain parental/carer permission for a child's image to be captured in digital photographs or videos and for what purpose involving their child as part of the school consent. Permission is asked on entry to the school and annually.
- Parental/carer consent ranges across the following purposes: the parent contact list, the weekly E-Newsletter, paper-based school marketing, online prospectus/websites and other online publications.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs. We also make sure photo file names/tags do not include full names to avoid accidentally sharing them in public facing material.
- Staff check the latest database in order to act properly on these various permissions.
- Any pupils shown in public facing materials are never identified and photo file names/tags do not include names to avoid accidentally sharing them.
- All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored.
- At LCS, no member of staff will ever use their personal phone to capture photos or videos of pupils
- Photos are stored on school devices and on the school's managed G Suite in line with the retention schedule of the school Data Protection Policy.
- Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.
- At special school events e.g. performances/sports days, photos and video may be taken by parents but may only be used for private use, and must not be shared publicly on any social networks. No live streaming is allowed. We give reasons for this and reminders whenever an event takes place.
- On school trips, photos and videos may not be taken by parents. We give reasons for this and reminders whenever they come on the trip as a volunteer.
- Pupils are taught about how images can be manipulated in their online safety curriculum and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work.
- Pupils are also encouraged to think about their online reputation and digital footprint.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make their personal information public.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), which reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

7. Social Media

We manage and monitor our social media footprint carefully to know what is being said about the school and

to respond to criticism and praise in a fair, responsible manner.

Nicola Collett-White is responsible for managing our online presence, e.g checking our Wikipedia and Google reviews. She follows guidance in the Internet Centre online-reputation management document [here](#).

See the Social Media policy for more detail.

Staff, pupils and parents social media presence

We expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face. This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents/carers have a concern about the school, we urge them to contact us directly and in private to resolve the matter, and we also have an email address devoted specifically to 'complaints'. When making complaints, our complaints procedure should be followed.

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults. Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when.

The school asks parents/carers not to use social media channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and pupils. Staff are asked not to 'friend' parents in the school community on social networks unless the relationship is pre-existing and completely separate and distinct from the parent/staff relationship.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on digital images and video and permission is sought before uploading photographs, videos or any other information about other people.

8. Device Usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Storage, syncing and access on school owned digital devices

If the device is accessed with a school owned account:

- All devices have school created accounts and all apps and file-use is in line with this policy. No personal elements may be added to this device
- The passcode for access to a school device must always be known by the network manager and must be regularly changed

Handling hardware around the school

- Pupils will only carry three pieces of any hardware at a time.
- Where possible staff will model best practice of hardware handling.
- Ways in which to responsibly carry and care for all forms of hardware are taught through the computing curriculum and embedded into the culture of the school.
- Digital leaders are trained specifically in modelling, taking care of and then also teaching best practice for carrying hardware around the school.

Personal devices for staff

- Personally owned mobile devices brought into school are entirely at the staff members', students', parents' or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of personally owned mobile devices brought into the school.
- Teachers with personally owned mobile devices are only permitted to use them in a room where no pupils are present.
- Teachers' personally owned mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- The recording, taking and sharing of images, video and audio on any personal mobile device is not allowed.
- The school reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobile devices may be searched at any time as part of routine monitoring.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Staff will be issued with a school phone or another school digital device where contact with parents or carers is required or photos are to be taken for professional purposes, for instance for off-site activities (e.g. school trips).
- Staff are allowed to use their personally owned mobile devices to work remotely outside the school setting (e.g. check Google Suite/Purplemash), however they must adhere to the LCS Staff Code of Conduct for online communication (see appendices), must make sure they log out of these accounts/apps after use and must make sure their personally owned devices are locked with strong passwords.
- When accessing school approved accounts/apps (e.g. Purplemash/Google Suite/Evidence Me), staff will not download anything onto their own digital device e.g. photos or videos of children.
- In an emergency (such as a lock down) where a staff member does not have access to a school-owned device, they should use their own device and hide their own mobile number for confidentiality purposes and then report the incident to the Head Teacher and the OSL.
- If a member of staff breaches the school policy on personally owned mobile devices then disciplinary action may be taken.
- If a staff member needs to connect to the school's wifi, permission is sought from the OSL/DSL, Head/DDSL or Computing Lead, and access is given to a wifi network.

Personal Devices for Pupils

- Where we mention 'mobile devices' below, we include within that category any wearable technology that connects to the internet (e.g. Apple watches, SpaceTalk watches).
- Personally owned mobile devices brought into school are entirely at the pupils' and parents/carers' own risk. The school accepts no responsibility for the loss, theft or damage of personally owned mobile devices brought into the school.
- The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- All pupil's mobile devices will be handed in to the office should they be brought into school where they will be safely stored for the duration of the school day.
- Pupils can collect their mobile devices at the end of the school day and on exit from the building.
- In line with DfE guidance '[Searching, screening and confiscation: advice for schools](#)', LCS has statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices,

for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

- Any pupil's mobile device that comes into school and is not declared at first will be confiscated.
- No pupil device is allowed connectivity to the school internet except during remote teaching when a key worker pupil brings in their own device due to shortage of devices at school. In this case, they are allowed to access the school wireless internet network for school-related internet use within the framework of the acceptable use policy. All such use is monitored.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- If a pupil breaches the school policy on personally owned mobile devices then disciplinary action may be taken.

Personal devices for parents/carers

- Parents are encouraged to leave their phones in their pockets when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.
- When at specific school events such as sports day or school performances, parents/carers are allowed to film and take photos of children. They are allowed to share these photos within the school community and are asked not to share them with the general public who they do not know. We verbally remind parents/carers of these things as a specific school event starts.
- Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.
- No parent device is allowed connectivity to the school wifi.

Personal Devices for volunteers, contractors and governors

- Volunteers, contractors and governors are encouraged to leave their phones in their pockets.
- Under no circumstances should they be used in the presence of children or to take photographs or videos.
- If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Head Teacher should be sought and this should be done in the presence of a staff member.
- Occasionally a visitor may need to connect to the school's wifi. In this situation, permission is sought from the OSL/DSL, Head/DDSL or Computing Lead, and access is given to a guest wifi network which is separate from the one the children access.

Trips/events away from school

- For school trips/events away from school, teachers will be issued a school phone and this number used for any authorised or emergency communications with pupils and parents/carers. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Head Teacher.
- Teachers using their personal phone in an emergency (e.g. lock down) will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Policy approved: Katie Vivyan (DSL/OSL) & Nicola Collett-White (Head Teacher/DDSL) Policy approved by the Governing Board: September 2025

Review date: September 2026

Contents of Appendices

Appendix A- Roles

Appendix B- Key Stage 1 Acceptable Use Agreement

Appendix C- Key Stage 2 Acceptable Use Agreement

Appendix D- EYFS Acceptable Use Agreement

Appendix E- Staff and Governor Acceptable Use Agreement

Appendix F- Guidance for Parents, Visitors & Contractors

Appendix G- How specific infringements will be handled – Sanctions etc.

Appendix H- Example of letter sent to parents if inappropriate material

Appendix A- Roles

Please read the relevant roles and responsibilities from the following pages:

All school staff must read the “All Staff” section as well as any other which are relevant to specialist roles.

Roles:

- All staff
- Headteacher
- Designated Safeguarding Lead/Online Safety Lead
- Governing Body, led by Online Safety/Safeguarding Link Governor
- PSHE/RSHE Lead
- Computing Lead
- Network Manager/Technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils
- Parents/carers
- External groups

All Staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school’s main safeguarding policy, the staff code of conduct handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

They must report any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the DfE standards for filtering and monitoring and play their part in feeding back to the DSL about overblocking, gaps in provision or pupils bypassing protections. All staff are responsible for the physical monitoring of pupils’ online devices during any session/class they are working within.

Headteacher - Nicola Collett-White

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee and support the activities of the DSL and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (see LGfL’s template with suggested questions at [onlinesafetyaudit.lgfl.net](https://www.lgfl.net/online-safety-audit))
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance.
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures.
- Ensure ALL governors undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the

nature and effectiveness of the school's arrangements.

- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards- through regular liaison with technical colleagues and the DSL- in particular understand what is blocked and allowed for whom, when and how as per KCSIE.
- Liaise with the DSL on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Support the DSL and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguardings (see remotesafe.lgfl.net)
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.
- Ensure the school website meets statutory requirements.

Designated Safeguarding Lead- Katie Vivyan

Key responsibilities:

- The DSL should "take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).
- Ensure "An effective whole school approach to online safety" as per KCSIE.
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring.
- As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engines. Our current search engine is Google Chrome.
- Where online safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. RSHE), ensure there is a regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused.
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.
 - This must include filtering and monitoring and help them to understand their roles.
 - All staff must read KCSIE Part 1 and all those working with children also Annex B.
 - Cascade knowledge of risks and opportunities throughout the organisation.
- Ensure that ALL governors undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).
- Work with the headteacher, DPO and governors to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training."
- Review and update this policy, other online safety documents (e.g. Acceptable Use agreements) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Receive regular updates about online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety is embedded across the curriculum in line with the statutory RSHE guidance (we use UKCIS framework '[Education for a Connected World](#)- 2020 edition') and beyond, in wider school life.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents (parentsafe.lgfl.net)

- Communicate regularly with SLT and the safeguarding governor to discuss current issues (anonymised), review incident logs and filtering logs and discuss how filtering and monitoring work have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident on My Concern.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site.
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and do not dismiss it as banter (including bullying).

Governing body, led by Online Safety/Safeguarding Link Governor - Lizzie Price and Filtering and Monitoring Governor - Mike Burden

Key responsibilities (quotes taken from KCSIE)

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) [Online Safety in schools and colleges: Questions from the Governing Board](#)
- Undergo (and signpost all other governors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated.
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards (there is guidance for governors at [safefiltering.lgfl.net](#)).
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring).
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology.

PSHE/RSHE Lead - Nicola Collett-White

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from latest trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum.
- Focus on the underpinning knowledge and behaviours outlined in 'Teaching Online Safety in Schools' in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should be included on the school website.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing Lead - Stephen Watson-Lowries

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging

within Computing.

- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Subject leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:

- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike.

- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context.

- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.

- Ensure subject specific action plans also have an online safety element.

Technician – Krzysztof Jurek with Hextrio

Key responsibilities:

- As listed in the 'all staff' section

- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- Work closely with the DSL/OSL/DPO to ensure that school systems and networks reflect school policy and they understand the consequences of existing services and of any changes to these systems e.g. access to personal and sensitive records/data, web filtering settings, sharing permissions for files on cloud platforms etc.

- Support DSL and SLT to carry out an annual online safety audit as now recommended in KCSIE.

- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL/OSL

- Maintain up-to-date documentation of the school's online security and technical procedures.

- To report online-safety related issues that come to their attention in line with school policy.

- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

- Oversee and work with other providers who manage certain systems e.g. Google

- Oversee and manage appropriate anti virus packages and mobile management solutions; Sophos Central, Mosyle, Apple School Manager, EXA networks, Server, G Suite services

Data Protection Officer - Amy Roseveare

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cyber security policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.

- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

- Note that retention schedules for safeguarding records may be required to be set as 'Very long-term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records. You should check the requirements in your area.

- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and contractors (including tutor)

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP)

- Report any concerns, no matter how small, to the designated safety lead.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy.

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental acceptable use policy (AUP), read the pupil AUP and encourage their children to follow it.

Appendix B– KS1 Acceptable Use Policy

These statements are on the Key Stage 1 acceptable use agreement and must be signed by child and parent.

AUP review date: August/September 2025

Date of next review: August/September 2026

Who has reviewed this: Katie Vivyan (DSL/OSL)

I will:

- Always ask a teacher or suitable adult if I want to use the Chromebooks, iPads or cameras
- Only open activities that an adult has told or allowed me to use
- Only use websites that a teacher or adult has told me/allowed me to use -Tell my teacher immediately if I click on a website by mistake
- Tell an adult if I see something on a screen that upsets me, or I am unsure of -Keep my passwords safe and will never use someone else's
- Never share personal information online such as my address and birthday -Never communicate with strangers online
- Be kind to others and not upset or be rude to them
- Look after the school IT equipment and tell a teacher straight away if something is broken or not working properly

Child's name: _____ Year group: _____

Signature of child: _____ Date: _____

I have discussed this with my child at home and agree to this acceptable use agreement. My child and I understand that if the agreement is broken in some way, there will be consequences which may include a period of time where they are not allowed to use school computing equipment.

Signature of parent: _____ Date: _____

Appendix C– Key Stage 2 Acceptable Use Policy

The form must be completed by parent and pupil before children can use the school internet and computing equipment.

AUP review date: August/September 2025

Date of next review: August/September 2026

Who has reviewed this: Katie Vivyan (DSL/OSL)

I will:

- Always use the school's IT systems and the internet responsibly and for educational purposes only
- Only use the school's IT systems and the internet a teacher or suitable adult is present, or with their permission
- Keep my username and passwords safe and not share these with others -Keep my private information safe at all times and not give my name and other personal details to anyone without permission from my parent/carers or teacher -Tell a teacher or other member of staff immediately if I find any material which might upset, distress or harm me or others
- Not share personal information such as phone numbers, home addresses and names
- Understand that in order to keep me and others safe, I know that the school can check my files and online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- Understand that in order to keep me and others safe, I know that the school can check my files and online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- Respect computing equipment and will immediately notify an adult if I notice something is not working correctly or is damaged
- Use all communication tools such as Google classroom, email and blogs carefully and I will not use any inappropriate language online.
- Before I share, post or reply to anything online, I will T.H.I.N.K -
T: Is it true?
H: Is it helpful?
I: Is it inspiring?
N: Is it necessary?
K: Is it kind?
- Understand that if I behave negatively whilst using tech towards other members of the school, my parents/carers will be informed and appropriate actions will be taken.

-For Year 6 only

If I bring a personal mobile phone or other personal electronic device, I will hand it straight to the office when I arrive

If I bring a personal mobile phone or other personal electronic device, I will use it responsibly.

Child's name: _____ Year group:

Signature of child: _____ Date: _____

I have discussed this with my child at home and agree to this acceptable use agreement. My child and I understand that if the agreement is broken in some way, there will be consequences which may include a period of time where they are not allowed to use school computing equipment.

Signature of parent: _____ Date: _____

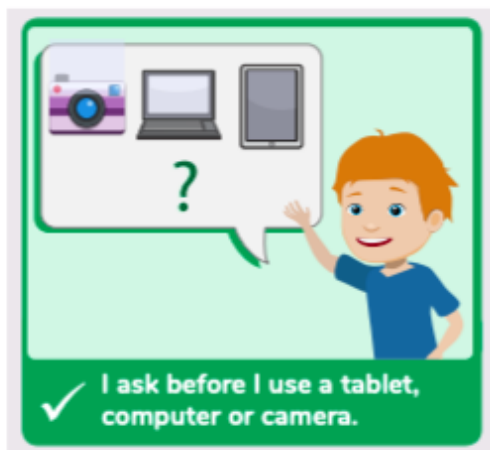
Appendix D - ER/R Acceptable Use Policy

AUP review date: August/September 2025

Date of next review: August/September 2026

Who has reviewed this: Katie Vivyan (DSL/OSL)

Early Reception and Reception Acceptable User agreement



Name of child: _____

Class: _____

I have discussed this with my child at home and agree to this acceptable use agreement.

Signed: _____ Date: _____

Name: _____

Appendix E – Staff and Governor Acceptable Use Policy

AUP review date: August/September 2025

Date of next review: August/September 2026

Who has reviewed this: Katie Vivyan (DSL/OSL)

1. I have read and understood the LCS Online Safety Policy in full and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead, Katie Vivyan (if by a child) or Head Teacher, Nicola Collett-White (if by an adult).
3. I understand the responsibilities listed for my role in the school's Online Safety Policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these. 4. I understand that Internet and devices used in school, and use of school-owned devices, networks and cloud platforms out of school, may be subject to filtering and monitoring. These should be used in the same manner as when in school.
5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same.
7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety Policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.
8. I understand the importance of upholding my online reputation, that of the school and of the teaching profession, and I will do nothing to impair either. More guidance on this point can be found in this [Online Reputation](#) guidance for schools and in LCS social media guidance within the Online Safety Policy.
9. I understand that school systems and users are protected by security, monitoring and filtering services, so my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, may be monitored/captured/viewed by these systems and/or relevant/authorised staff members.
10. I agree to adhere to all provisions of the LCS Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the technician and the OSL if I suspect a breach. I will not store school-related data on personal devices, storage or cloud platforms. USB keys should be used sparingly, and need to be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
11. I will use school devices and networks/internet/platforms/other technologies for school business and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring, will look after devices loaned to me, and will notify the school of "significant personal use" as defined by HM Revenue & Customs.
12. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school (see LCS Prevent Policy).
13. I understand and support the commitments made by pupils/students, parents/carers and fellow staff, governors and volunteers/visitors/contractors in their Acceptable Use Policies/safeguarding leaflets and will report any

infringements in line with school procedures.

14. I will follow the guidance in the Online Safety Policy for reporting incidents but also any concerns I might think are unimportant.
15. I have read and understood the 'Artificial Intelligence Policy' and will adhere to it.
16. I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

User signature

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety/safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by the Head Teacher, Nicola Collett-white

I approve this user to be allocated credentials on all school systems as relevant to their role.

Signature: _____

Name: _____



GUIDANCE FOR VISITORS TO LCS

SAFEGUARDING

- We are committed to providing a safe and secure environment for all children, staff and visitors, both offline and in a digital context.
- Safeguarding and promoting the welfare of children is the responsibility of the whole school community and we all have a part to play in keeping children at LCS safe. Therefore we expect all staff and visitors to be aware of and adhere to our Safeguarding Policy and Online Safety Policy (please ask the office for full copies if you require).
- All visitors to London Christian School must wear a visitor badge. Any adults without a visitor badge will be challenged.
- In addition to contributing to the safety of children, it is important to remember to keep yourself safe. Our actions can sometimes be perceived in a way that was not intended. The following guidelines are provided for the safety of all. Observing simple precautions can prevent potentially damaging situations. Awareness and common sense have a very important role to play.

WHAT TO DO

If a child discloses sensitive information to you:

- Listen. Ask open ended questions. Offer reassurance and stay calm. Do not promise to keep secrets. Do not ask leading questions.
- Do not physically examine children or ask them to act out what happened to them. Ensure that any further discussion is moved to a professional and child free environment.
- Record what has been said, noticed or witnessed. Explain that you will need to share this information as part of your duty to protect children.
- Be discreet. Speak only to those who 'need to know'.
- Assume 'it could happen here'. If you are unsure about a concern or action seek the advice of the Designated Safeguarding Lead or Deputy.

WHO DO YOU TELL?

If a child discloses sensitive information to you, or you have concerns about a child's safety during your visit, act quickly and share the information with the **Designated Safeguarding Lead/Online Safety Lead or Deputy Designated Safeguarding Lead at LCS (contact details below)**. It is your responsibility to alert the Safeguarding Leads if you suspect, hear or observe any concerns about a child.



Designated Safeguarding Lead
Online Safety Lead: Miss Katie Vivyan
Deputy Head Teacher
kvivyan@londonchristianschool.com
020 3130 6430



Deputy Designated Safeguarding Lead
Miss Nicola Collett-White
Head Teacher
ncollett-white@londonchristianschool.com
020 3130 6430

Other Safeguarding Contacts Chair of Governors | Rev'd Chris Fishlock | 020 3130 6430

FIRE SAFETY

- In the event of a fire, please proceed in a timely and calm manner to the main front doors and proceed to assemble in Tabard Gardens (turn right outside of the school and proceed to the end of the road).

ACCEPTABLE USE OF MOBILE PHONES AND ELECTRONIC DEVICES

- Please keep mobiles in your pocket and refrain from using personally owned mobile devices when children are present or to record videos, audio files or photos of children unless in a performance/special event where you will be given further guidance from the Headteacher.
- The school Wi-fi network is monitored and accessed by limited authorised password protection only. This guidance must be read and agreed upon before access is granted and permission must be sought from the OSL/DSL, Head/DSL or Computing Lead. Internet use must take place in the presence of a member of staff.
- You must report any suspected unsafe use of technology by anyone to a member of staff
- You must support the school in promoting online safety and data protection, and you must model good practice
- Information about the school or members of its community that you gain as a result of your visit must not be shared in any way or on any platform except where relevant to the purpose of your visit and agreed in advance with the school.

DATA PROTECTION

- We use CCTV monitoring as part of maintaining physical security on our premises and is clearly signposted
- LCS is committed to protecting personal data by collecting, processing and sharing data in accordance with current Data Protection Law. You can find our Privacy Notice on our website or ask for a copy from the school office.
- **By having signed the Visitor Book on your entry to the school, you are saying that you have read, understood and agreed to this policy. If you have any questions about this, please do speak to someone in the office.**

Appendix G: How specific infringements will be handled – Sanctions etc.

We recognise all individual cases of misconduct are complex and unique but below is an attempt to show clear consequences for specific misconduct. Whenever a pupil or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the LCS management and takes into account associated disciplinary policies.

Pupils

Category A Infringements	Possible Sanctions
● Use of non-educational sites during lessons ● Unauthorised use of email ● Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends ● Use of unauthorised instant messaging / social networking sites	Refer to OSL/DSL Record in the Online Safety Incident book, decide if a safeguarding concern sheet must be filled out and how the school's safeguarding policy is followed.
Category B Infringements	Possible Sanctions
● Continued use of non-educational sites during lessons after being warned ● Continued unauthorised use of email after being warned ● Continued unauthorised use of mobile phone (or other new technologies) after being warned ● Continued use of unauthorised instant messaging/chat rooms, social networking sites, NewsGroups ● Use of file sharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc ● Trying to buy items online ● Accidentally corrupting or destroying others' data without notifying a member of staff of it ● Accidentally accessing offensive material and not logging off or notifying a member of <u>staff of it</u>	Refer to OSL/DSL Record in the Online Safety Incident book, decide if a safeguarding concern sheet must be filled out and how the school's safeguarding policy is followed. Escalate to: Removal of Internet access rights for a period / removal of phone until end of day / contact with parent / time out
Category C Infringements	Possible Sanctions
● Deliberately corrupting or destroying someone's data, violating privacy of others or posting inappropriate messages, videos or images on a social networking site ● Sending an email or chat message that is regarded as harassment or of a bullying nature (one-off) ● Trying to access offensive or pornographic material (one-off) ● Purchasing or ordering of items online ● Transmission of commercial or advertising material	Refer to OSL/DSL Record in the Online Safety Incident book, decide if a safeguarding concern sheet must be filled out and how the school's safeguarding policy is followed. Escalate to: Head Teacher / removal of Internet access rights for a period / removal of phone until end of day / contact with parent Other safeguarding actions

	If inappropriate web material is accessed: ensure appropriate technical support filters the site and follow Safeguarding Policy
Category D Infringements	Possible Sanctions
- Continued sending of emails or chat messages regarded as harassment or of a bullying nature after being warned - Deliberately creating, accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent - Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 - Bringing the LCS name into disrepute	Refer to OSL/DSL Record in the Online Safety Incident book, safeguarding concern sheet must be filled out and school's safeguarding policy is followed. Escalate to: Head Teacher/ contact with parents/ possible fixed term or permanent exclusion Other safeguarding actions If inappropriate web material is accessed: ensure appropriate technical support filters the site and follows safeguarding policy. Secure and preserve any evidence Inform the sender's email service provider. Liaise with relevant service providers/ instigators of the offending material to remove Report to Police / CEOP where child abuse or illegal activity is suspected

Staff

Category A Infringements (misconduct)	Possible Sanctions
- Excessive use of the Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc - Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored - Not implementing appropriate safeguarding procedures - Any behaviour on the World Wide Web that compromises the staff member's professional standing in the school and community - Misuse of first level data security, e.g. wrongful use of passwords - Breaching copyright or license e.g. installing unlicensed software on network	Refer to Head Teacher Escalate to: Head Teacher/ warning given
Category B Infringements (misconduct)	Possible Sanctions
- Serious misuse of, or deliberate damage to, any school computer hardware or software - Any deliberate attempt to breach data	Refer to Head Teacher Escalate to: Head Teacher/governors/suspension or

protection or computer security rules • Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Accessing websites advocating violent extremism • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 • Bringing the school name into disrepute	dismissal Other safeguarding actions: Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. Instigate an audit of all ICT equipment by an outside agency, CLC, to ensure there is no risk of pupils accessing inappropriate materials in the school. Identify the precise details of the material. Escalate to: report to LA /SSCP, Human Resources, Report to Police / CEOP where child abuse or illegal activity is suspected.
If a member of staff commits an exceptionally serious act of gross misconduct	
The member of staff should be instantly suspended. Normally, though, there will be an investigation before disciplinary action is taken for any alleged offence. In the first instance contact the LADO. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken. LCS would involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence.	
Child abuse images found	In the case of child abuse images being found, the member of staff should be immediately suspended and the police should be called. Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP) http://www.ceop.gov.uk/reporting_abuse.html http://www.iwf.org.uk

Appendix H: Example template for conversations

Video Games and keeping your child safe: Guidance to aid conversations with parents.

Dear Parent/Carer,

Child's name: _____ Class: _____

It has been brought to our attention that your child has been playing console games such as _____, even though the certification for this game is _____ based on International PEGI ratings.

London Christian School is committed to keeping our children safe and to promoting the safe, responsible use of the technologies. As such, we feel it is our responsibility to raise this particular issue as a concern.

1) Ratings denote the content and appropriateness of games

Since 2003 games have been age rated under the Pan-European Game Information (PEGI) system which operates in the UK and over 30 other countries of Europe, in addition, where a game showed realistic scenes of gross violence or sexual activity the game had to be legally classified and received one or other of the BBFC classification certificates given for videos/DVDs.

The PEGI system has been effectively incorporated into UK law and video games will be age rated at one or other of the above age levels; which you will find on video game sleeves. Ratings do not denote the difficulty or the enjoyment level of a game, but that it contains content suitable for a certain age group and above.

The PEGI age ratings will enable parents and carers to make an informed choice when buying a game for their children.

It is important to note that the 12, 16 and 18 age ratings are mandatory and that it is illegal for a retailer to supply any game with any of these ratings to anyone below the specified age. The age ratings 3 and 7 are advisory only.

An **18 Rated game** is applied when the level of violence reaches a stage where it becomes gross violence and/or includes elements of specific types of violence. **In general terms it is where the level of violence is so visually strong that it would make the reasonable viewer react with a sense of revulsion.**

2) Content Indicators

In addition to age ratings, video games will include indicators of the type of content and activities that the game includes in it. The descriptors are fairly self-explanatory but should be read in conjunction with the age rating given for a video game.

A violence descriptor with an 18 rated game will indicate a more extreme level of violence than a violence descriptor with a 12 rated game. Similarly a sex/nudity descriptor with a 12 rated game will probably indicate sexual innuendo but a sex/nudity descriptor with an 18 rated game will indicate sexual content of a more explicit nature.

3) Parental responsibility

We feel it is important to point out to parents the risks of underage use of such video games, so you can make an informed decision as to whether to allow your child to be subjected to such images and content.

- The PEGI ratings system helps you make informed decisions about which video games to choose for your family.
- A PEGI rating gives the suggested minimum age that you must be to play a game due to the suitability of the content.
- As parents you can take direct control of what games your children play at home, how they play them and for how long through parental controls on video game systems such as the Xbox or Playstation.
- Choosing and playing video games as a family is the best way to understand and enjoy them together.
- The stories, worlds and characters in video games offer playful ways to engage with a wide range of subjects and fuels creativity, interests and imagination.
- The recently relaunched www.askaboutgames.com website provides further information about video games ratings and offers real family stories and suggestions on how videogames can be a creative and collaborative experience for all the family.
- We also recommend that all parents visit the CEOP Think U Know website for more information on keeping your child safe online www.thinkuknow.co.uk

4) School support and action

London Christian School has a focussed Online Safety Day each year, as well as discussing online safety issues throughout the year in lessons and assemblies.

If you feel that you, or your child, needs further support in keeping your child safe on the internet, please make an appointment to see Katie Vivyan (Online Safety Lead and Designated Safeguarding Lead).

With thanks for your continued support,

Miss Katie Vivyan